CyberData

The IP Endpoint Company

VoIP Intercom Operations Guide

Part #*010935*

Document Part #*930242AB*
for Firmware Version *6.3.0*

CyberData Corporation
3 Justin Court
Monterey, CA 93940
(831) 373-2601

PoE VoIP Intercom Operations Guide 930242AB
Part # 010935

CyberData
The IP Endpoint Company

Technical Support

The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:
http://www.cyberdata.net/support/contactsupportvoip.html

Phone: (831) 373-2601, Ext. 333
Email: support@cyberdata.net
Fax: (831) 373-4193
Company and product information is at **www.cyberdata.net**.

Revision Information

Revision 930242AB, which was released on February 12, 2013 and corresponds to firmware version 6.3.0, has the following changes:

- Updates Section 1.6, "Product Specifications".
- Updates Section 2.1.6, "RTFM Button".

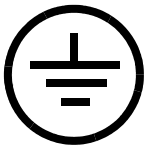
Important Safety Instructions

1. Read these instructions.
2. Keep these instructions.
3. Heed all warnings.
4. Follow all instructions.
5. Do not use this apparatus near water.
6. Clean only with dry cloth.
7. Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.
8. Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
9. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11. Only use attachments/accessories specified by the manufacturer.
12. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.
13. Prior to installation, consult local building and electrical code requirements.
14. **WARNING: The VoIP Intercom enclosure is not rated for any AC voltages!**

 GENERAL ALERT	Warning *Electrical Hazard:* This product should be installed by a licensed electrician according to all local electrical and building codes.

 GENERAL ALERT	Warning *Electrical Hazard:* To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.

Pictorial Alert Icons

	General Alert *This pictoral alert indicates a potentially hazardous situation. This alert will be followed by a hazard level heading and more specific information about the hazard.*
	Ground *This pictoral alert indicates the Earth grounding connection point.*

Hazard Levels

Danger: Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury. This is limited to the most extreme situations.

Warning: Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

Caution: Indicates a potentially hazardous situation which, if not avoided, could result in minor or moderate injury. It may also alert users against unsafe practices.

Notice: Indicates a statement of company policy (that is, a safety policy or protection of property).

The safety guidelines for the equipment in this manual do not purport to address all the safety issues of the equipment. It is the responsibility of the user to establish appropriate safety, ergonomic, and health practices and determine the applicability of regulatory limitations prior to use. Potential safety hazards are identified in this manual through the use of words Danger, Warning, and Caution, the specific hazard type, and pictorial alert icons.

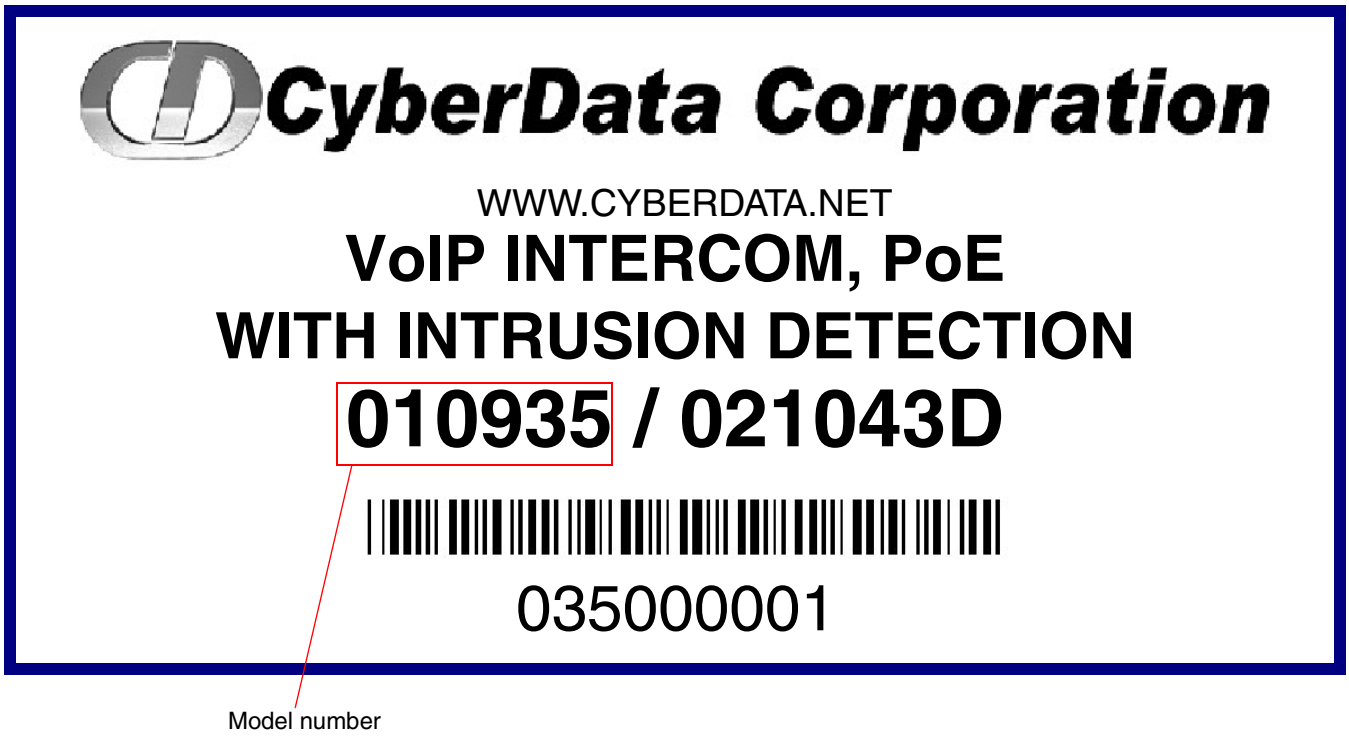
Contents

1 Product Overview

1.1 How to Identify This Product

To identify the VoIP Intercom, look for a model number label similar to the one shown in Figure 1-1. The model number on the label should be **010935**.

Figure 1-1. Model Number Label



1.2 Typical System Installation

The Voice-over-IP (VoIP) Intercom is a SIP endpoint designed to provide VoIP phone connectivity in a tamper proof and secure package.

Figure 1-2, Figure 1-3, and Figure 1-4 illustrate how the VoIP Intercoms can be installed as part of a VoIP phone system.

Figure 1-2. Typical Installation—Door Entry/Access Control

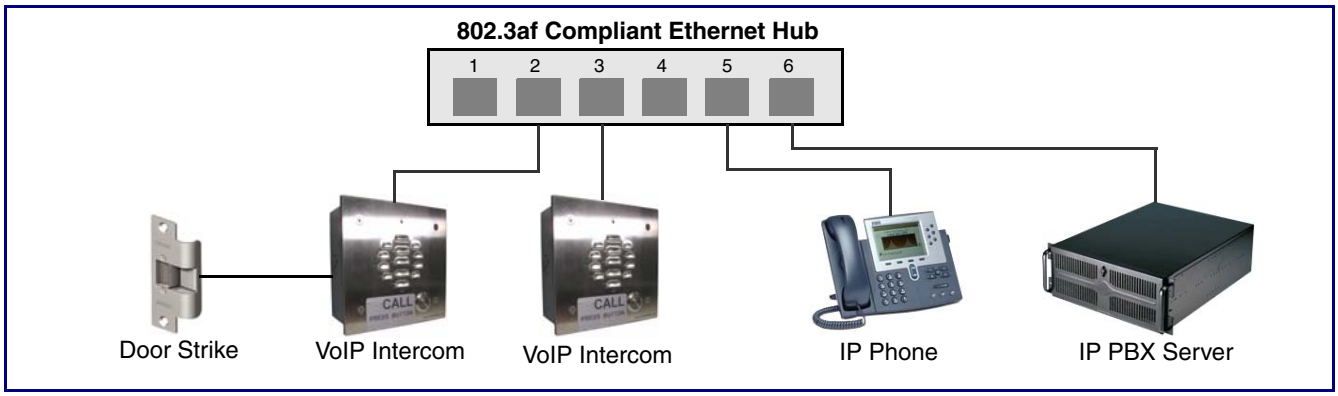


Figure 1-3. Typical Installation—Mass Notification

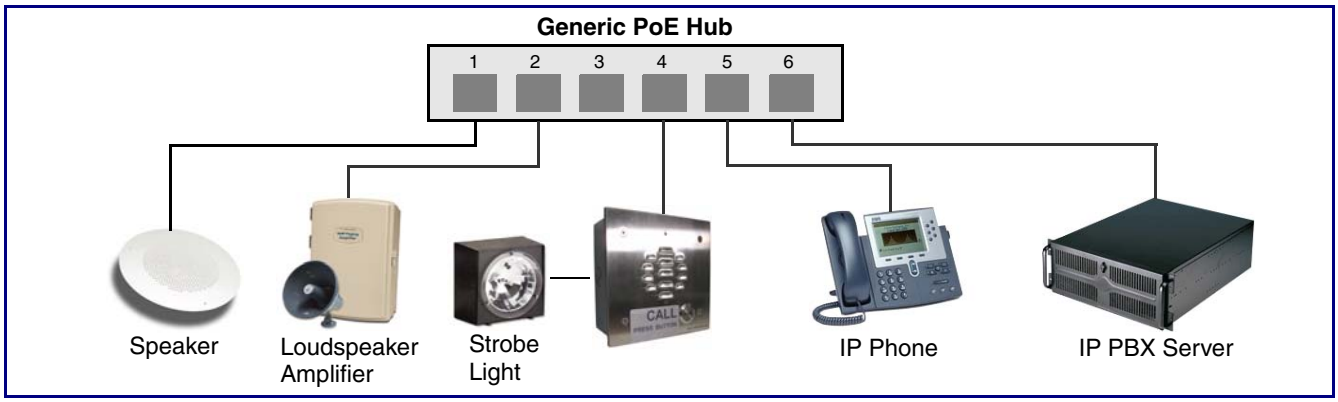
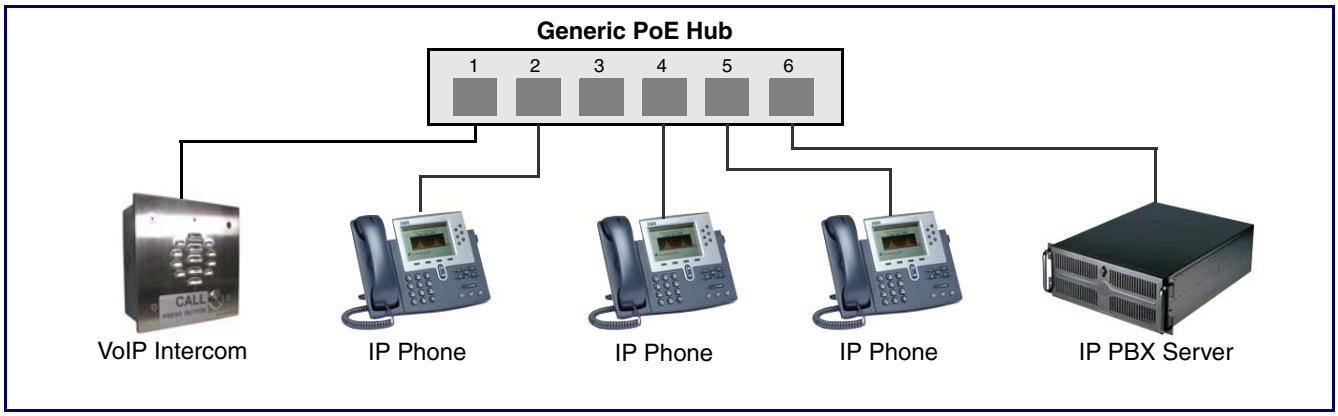


Figure 1-4. Typical Installation—Emergency Phone



Warning

Electrical Hazard: The VoIP Intercom enclosure is not rated for any AC voltages.

Warning

Electrical Hazard: This product should be installed by a licensed electrician according to all local electrical and building codes.

Warning

Electrical Hazard: To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.

1.3 Product Features

- *SIP*
- *Dual speeds of 10 Mbps and 100 Mbps*
- *802.3af compliant*
- *2 gang outlet box size*
- *Adaptive full duplex voice operation*
- *Network/Web management*
- *Network adjustable speaker volume adjustment*
- *Network configurable door or intrusion sensor settings*
- *Network configurable relay activation settings*
- *Dial Out Extension supports the addition of comma delimited pauses before sending additional DTMF tones*
- *Network configurable microphone input sensitivity adjustment*
- *Network downloadable product firmware*
- *Doubles as a paging speaker*
- *Call button*
- *Call activity indicator (light)*
- *Tamper proof design*
- *One dry contact relay for auxiliary control*
- *Autoprovisioning*
- *Configurable audio files*
- *Night Ringer*
- *Three year warranty*
- *Peer-to-peer capable*
- *Door closure and tamper alert signal*
- *Optional Torx screws with driver kit*

1.4 Supported Protocols

The Intercom supports:

- SIP
- HTTP Web-based configuration

  Provides an intuitive user interface for easy system configuration and verification of Intercom operations.
- DHCP Client

  Dynamically assigns IP addresses in addition to the option to use static addressing.
- TFTP Client

  Facilitates hosting for the Autoprovisioning configuration file.
- RTP
- RTP/AVP - Audio Video Profile
- Facilitates autoprovisioning configuration values on boot
- Audio Encodings

  PCMU (G.711 mu-law)

  PCMA (G.711 A-law)

  Packet Time 20 ms

1.5 Supported SIP Servers

Go to the following link to find the VoIP Intercom product page which will have information on how to configure the VoIP Intercom for various supported SIP servers:

http://www.cyberdata.net/support/server/index.html

1.6 Product Specifications

Category	Specification
Speaker Output	1 Watt Peak Power
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Power Input	PoE 802.3af compliant
	or +5 volts at 1000m
Operating Temperature	-10° C to 50° C (14° F to 122° F)
Payload Types	G711, A-law and µ-law
Regulatory Compliance	FCC Class A, UL 60950
Part Number	010935
Dimensions	5” x 5” x 2.5”
Weight	1.6 lbs./shipping weight of 2.2 lbs.
	(0.7 kg/shipping weight of 1.0kg)
Auxiliary Relay	1A at 30 VDC

1.7 Dimensions

Figure 1-5. Dimensions—Size of Unit With Case

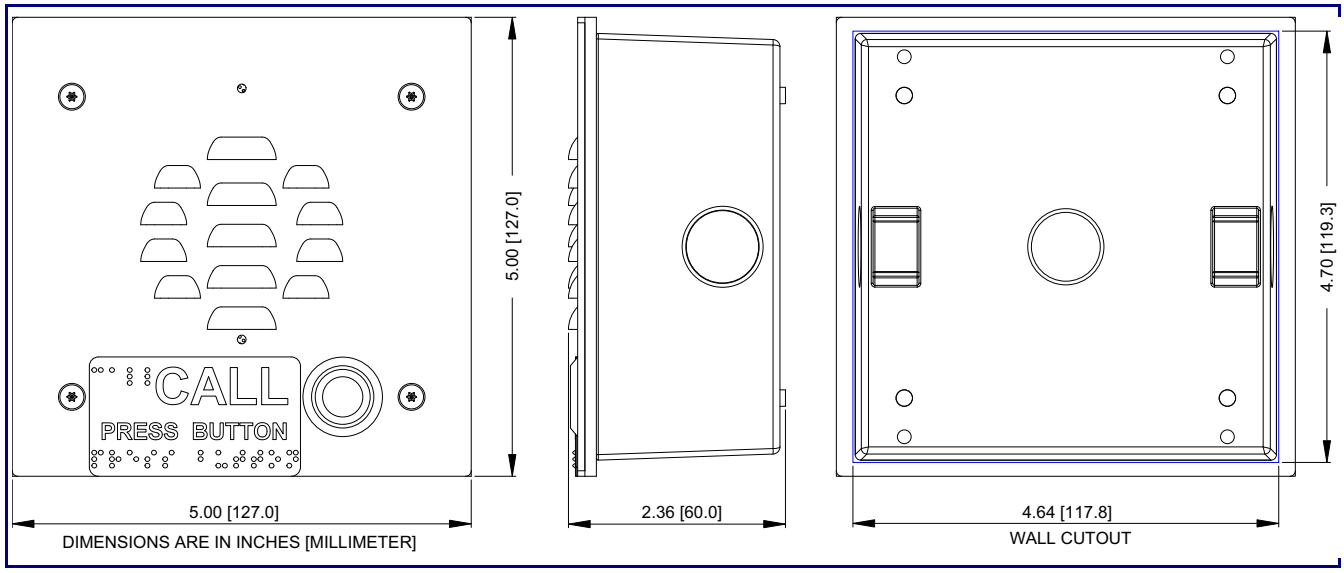
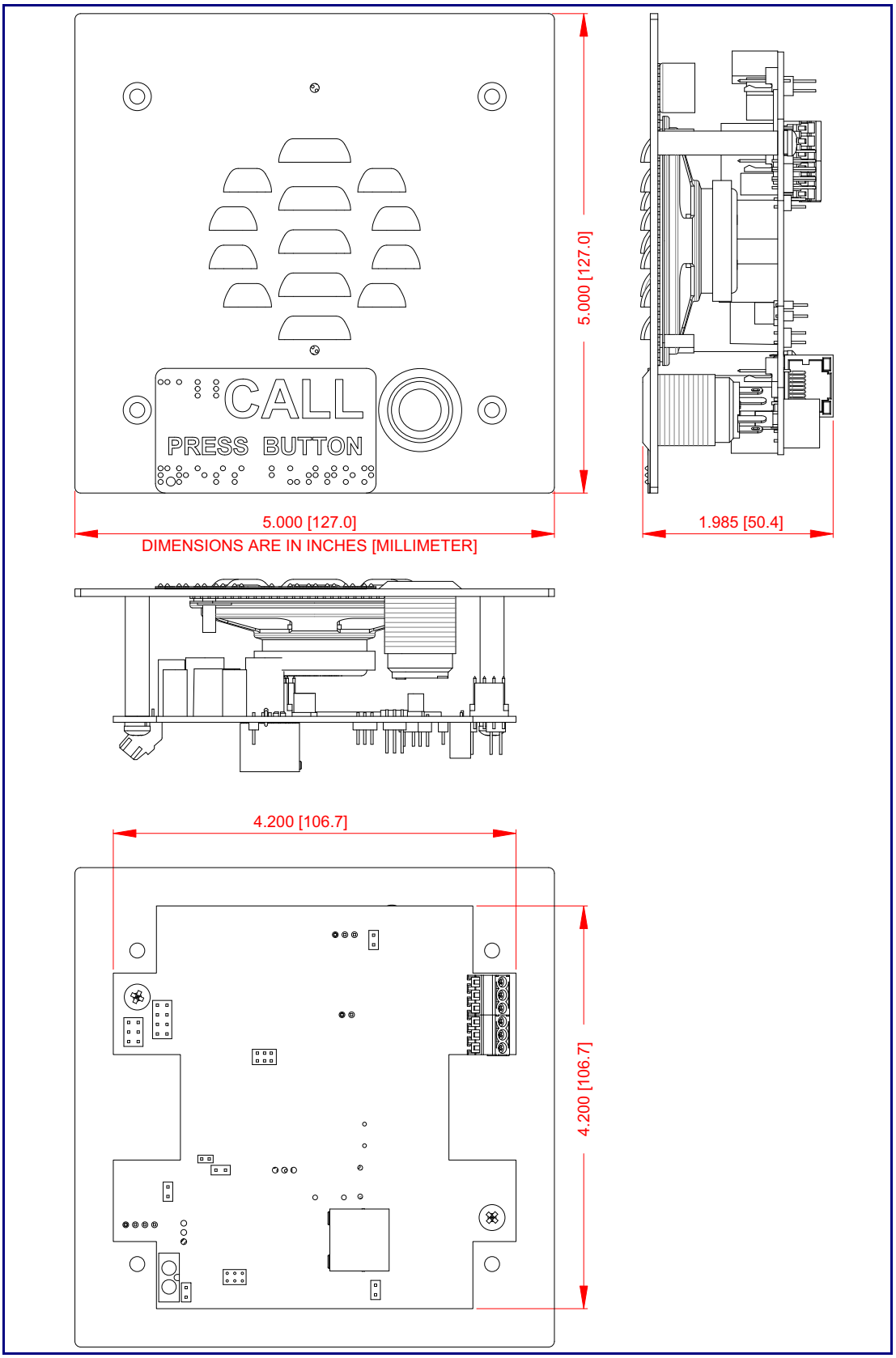


Figure 1-6. Dimensions—Size of Unit Without Gang Box

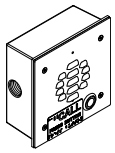


2 Installing the VoIP Intercom

2.1 Parts List

Table 2-1 illustrates the SiP VoIP and PoE Speaker parts.

Table 2-1. Parts List

Quantity	Part Name	Illustration
1	Intercom Assembly	
1	Installation Quick Reference Guide	
1	Intercom Mounting Accessory Kit	

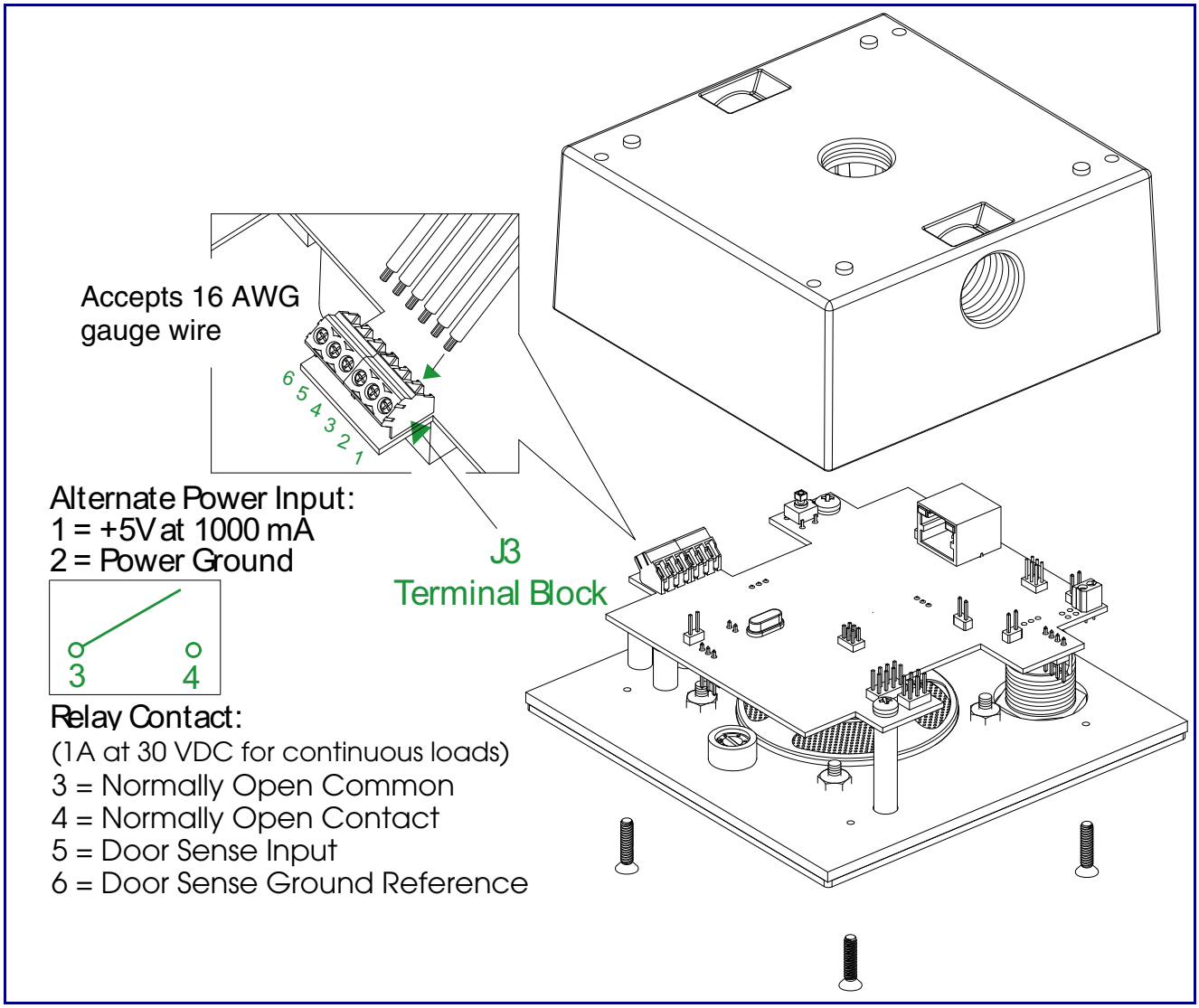
2.1 Intercom Setup

2.1.1 VoIP Intercom Connections

Figure 2-1 shows the pin connections on the J7 (terminal block). This terminal block can accept 16 AWG gauge wire.

Note As an alternative to using PoE power, you can supply 5 VDC at 1000 mA into the terminal block.

Figure 2-1. VoIP Intercom Connections



2.1.2 Connecting the Intercom to the Auxiliary Relay

Warning

Electrical Hazard: The VoIP Intercom enclosure is not rated for any AC voltages.

Warning

Electrical Hazard: This product should be installed by a licensed electrician according to all local electrical and building codes.

Warning

Electrical Hazard: To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.

Warning

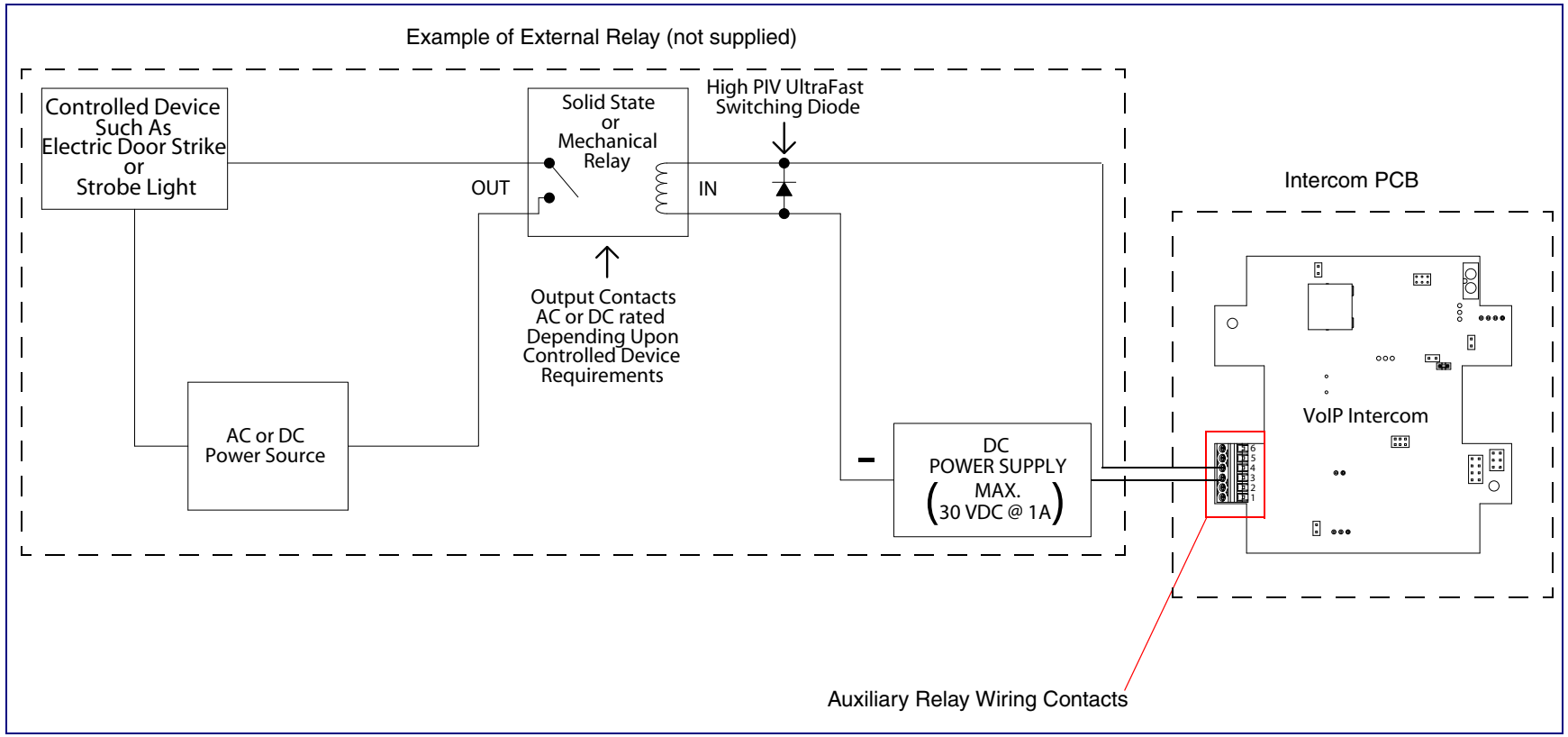
Electrical Hazard: The relay contacts are dry and provided for a normally open and momentarily closed configuration. Neither the alternate power input nor PoE power can be used to drive a door strike.

The VoIP Intercom incorporates an on-board relay which enables users to control an external relay for activating an auxiliary device such as an electric door strike (see Figure 2.1.2, "Connecting the Intercom to the Auxiliary Relay").

The Intercom relay contacts are limited to 1A at 30 VDC. The Intercom relay activation time is selectable through the web interface and is controlled by DTMF tones generated from the phone being called. The DTMF tones are selectable from the web interface as well.

Note The three digit code for the auxiliary relay must be sent in conformance with RFC2833 DTMF generation.

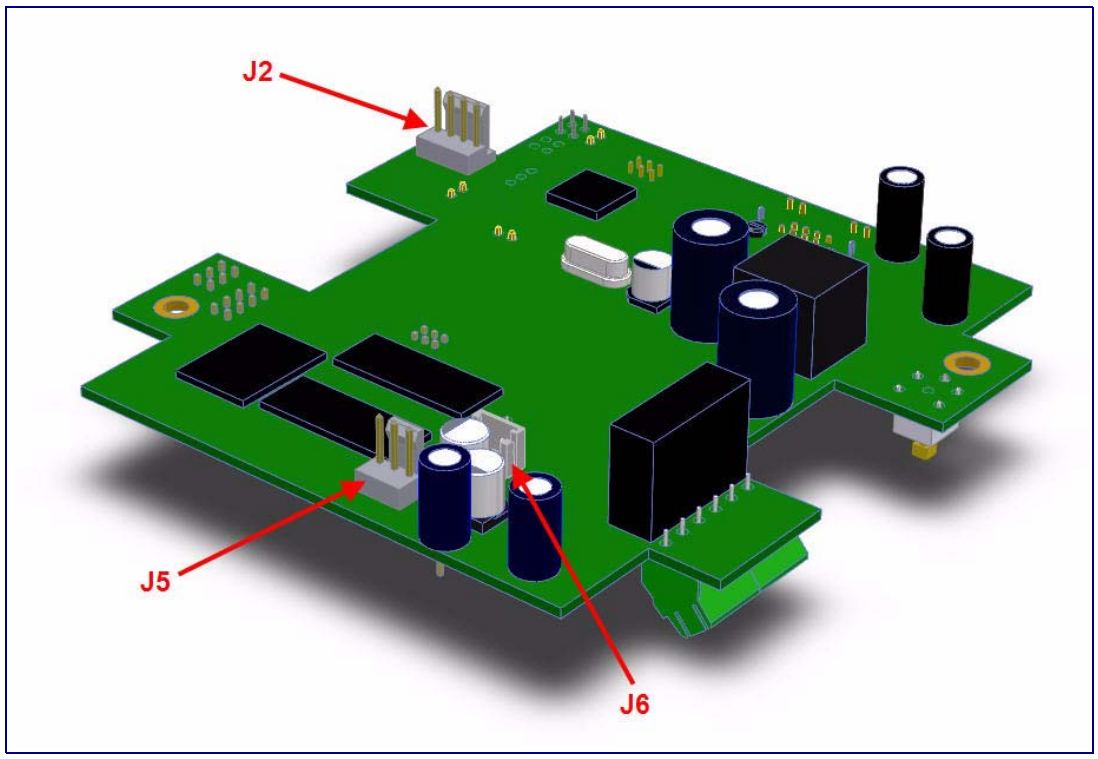
Figure 2-2. Auxiliary Relay Wiring Diagram



2.1.3 Identifying the VoIP Intercom Connectors

See the following Figures and Tables to identify the connectors and functions.

Figure 2-3. J2, J5, and J6 Connector Locations



.

Table 2-2. Connector Functions

Connector	Function
J2	Call Button. LED Interface
J5	Microphone Interface
J6	Speaker Interface

Figure 2-4. Connector Locations

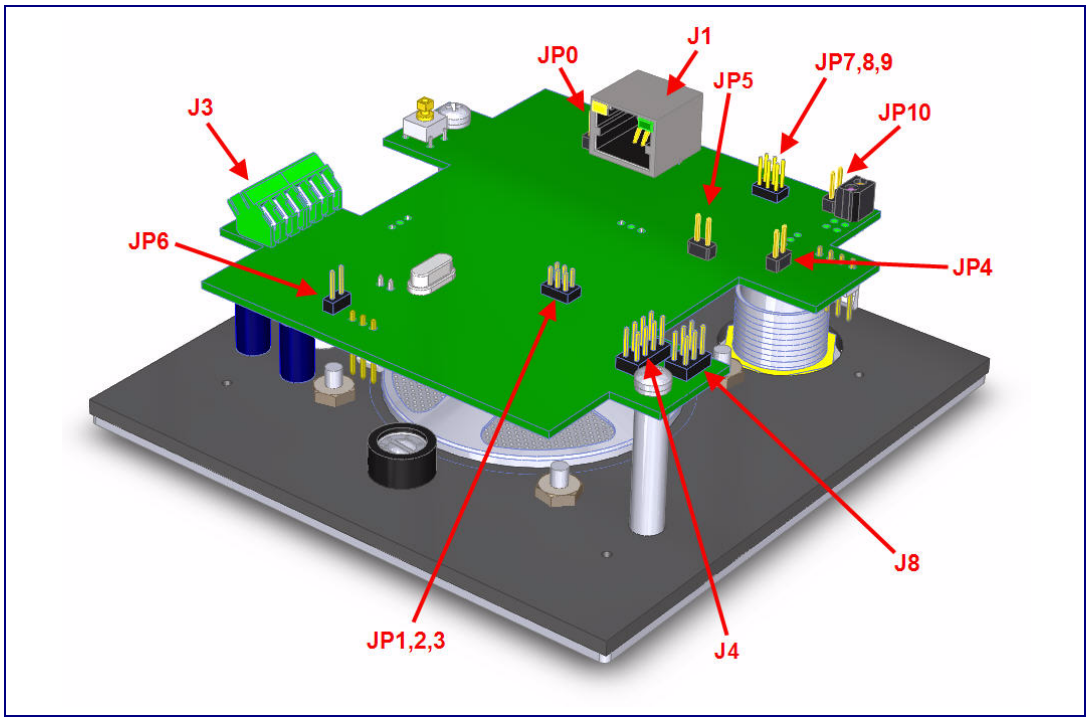


Table 2-3. Connector Functions

Connector	Function
J1	PoE Network Connection (RJ-45 ethernet)
J3	Terminal Block (see Figure 2-1)
J4	Factory Only
J8	Factory Only
JP0	Factory Only
JP1	Factory Only
JP2	Factory Only
JP3	Factory Only
JP4	Factory Only
JP5	Factory Only
JP6	Factory Only
JP7	Factory Only
JP8	Factory Only
JP9	Factory Only
JP10	Disables the intrusion sensor when installed.
SW1	RTFM (see Section 2.1.6, "RTFM Button")

2.1.4 Call Button and the Call Button LED

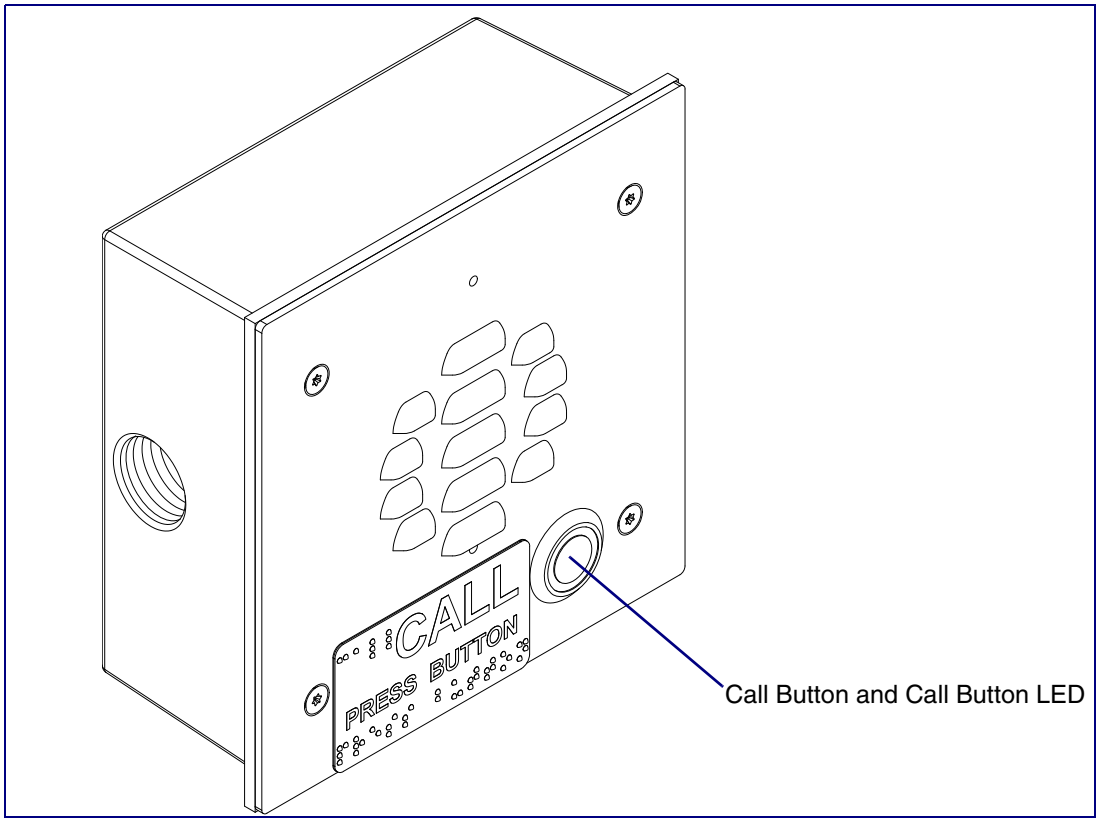
2.1.4.1 Calling with the The Call Button

- You may initiate a call by pressing the **Call** button.
- An active call is indicated by the Call Button LED blinking at one second intervals.
- The Intercom will automatically answer an incoming call.
- You can press the **Call** button to terminate an active call whether the call was an incoming call or a call that was initiated by you.

2.1.4.2 Call Button LED Function

- Upon initial power or reset, the Call Button LED will illuminate.
- When the software has finished initialization, the Call Button LED will blink twice.
- When a call is established (not just ringing), the Call Button LED will blink.
- On the **Device Configuration Page**, there is an option called **Button Lit When Idle**. This option sets the normal state for the indicator light. The Call Button LED will still blink during initialization and calls.
- The Call Button LED flashes briefly at the beginning of RTFM mode.

Figure 2-5. Call Button and Call Button LED

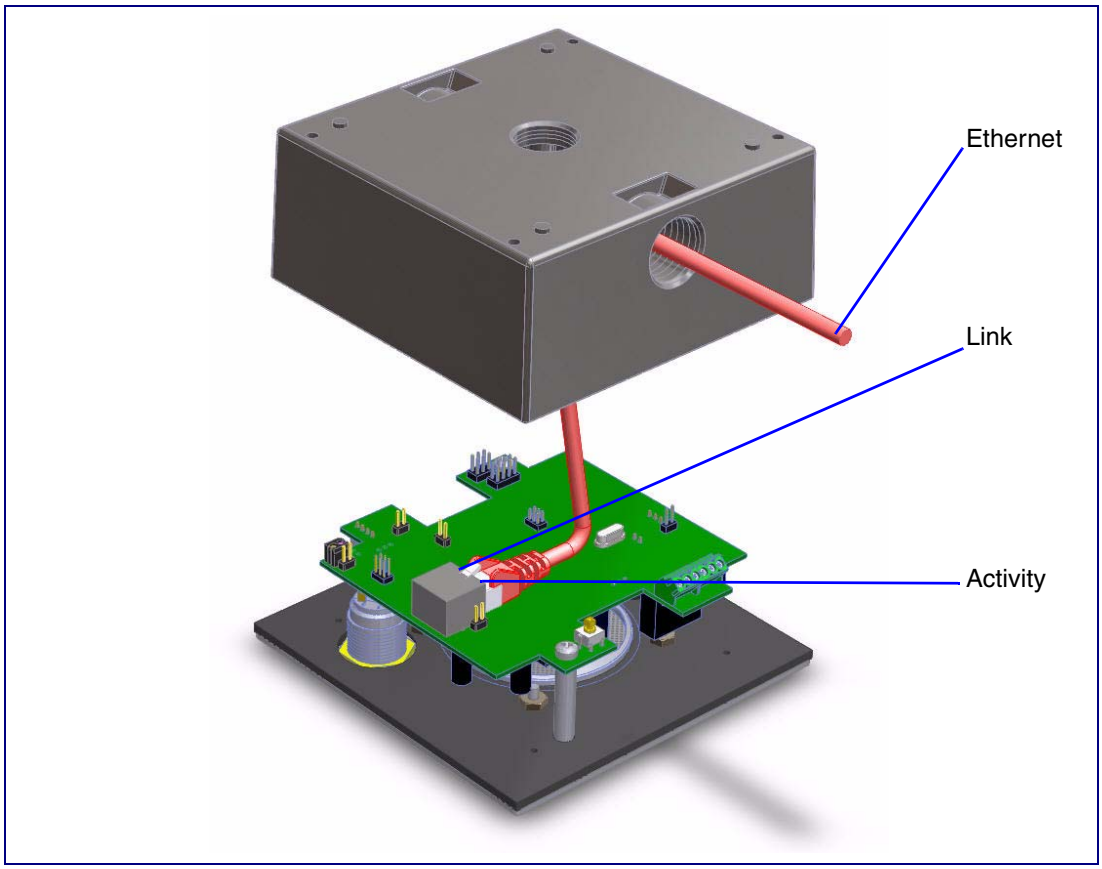


2.1.5 Network Connectivity, and Data Rate

When you plug in the Ethernet cable or power supply:

- The square, green **Link** light above the Ethernet port indicates that the network connection has been established (see Figure 2-6 and Figure 2-7). The Link light changes color to confirm the auto-negotiated baud rate:
- This light is yellow at 10 Mbps.
- It is orange at 100 Mbps.

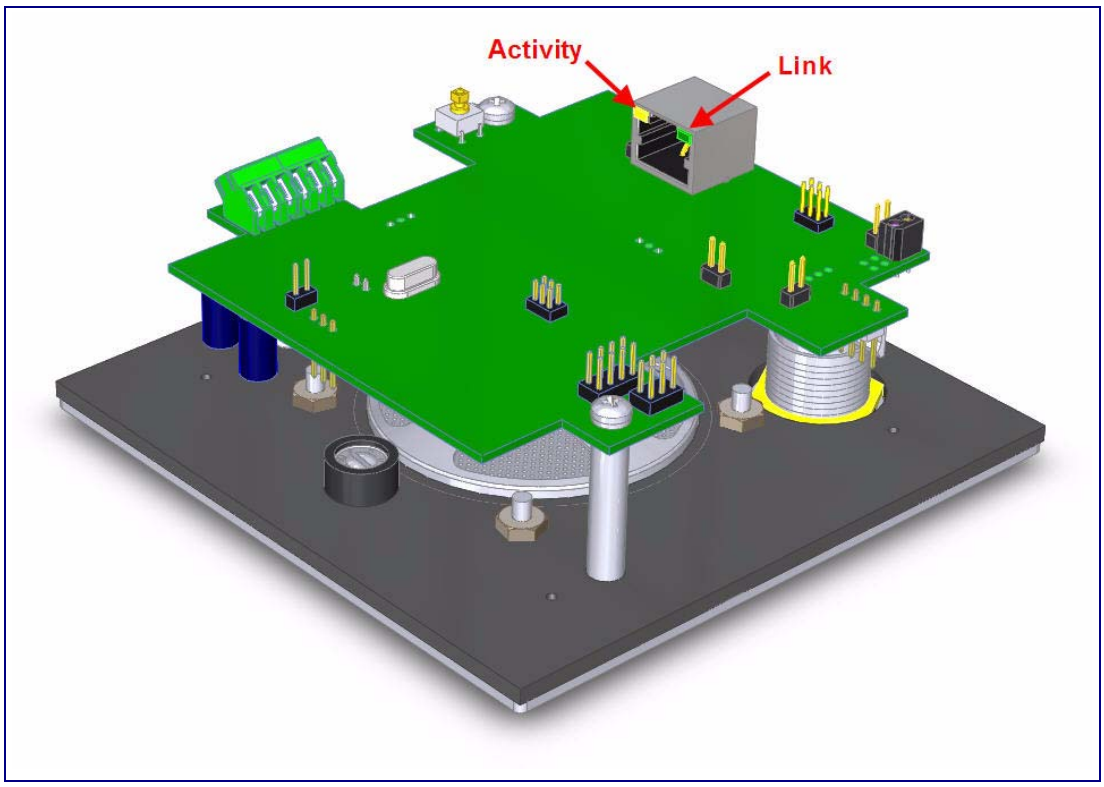
Figure 2-6. Network Connector Prior to Installation



2.1.5.1 Verify Network Activity

The square, yellow **Activity** light blinks when there is network activity.

Figure 2-7. Network Connector



2.1.6 RTFM Button

GENERAL ALERT

Caution

Your intercom will have either an RTFM button or two jumper pins labeled JP11 on the circuit board. If your intercom does not have an RTFM button, use JP11 for IP address announcement and factory reset functions. Intercoms with JP11 jumper pins instead of an SW1 switch correspond to part numbers 010935A, 010935B, 010935C, 010935D, and 010935E. You will need a jumper shunt to place over the JP11 jumper pins per the instructions below. Intercoms with an RTFM button correspond to part number 010935F.

When the Intercom is operational and linked to the network, use the Reset Test Function Management (RTFM) button (see **SW1** in Figure 2-8) or place a jumper shunt on the JP11 jumper pins (see **JP11** in Figure 2-9) on the Intercom board to announce and confirm the Intercom's IP Address and test the audio is working. Your intercom will have an RTMF button or a JP11 jumper but not both.

Note You must do these tests prior to final assembly.

Figure 2-8. RTFM Button (SW1)

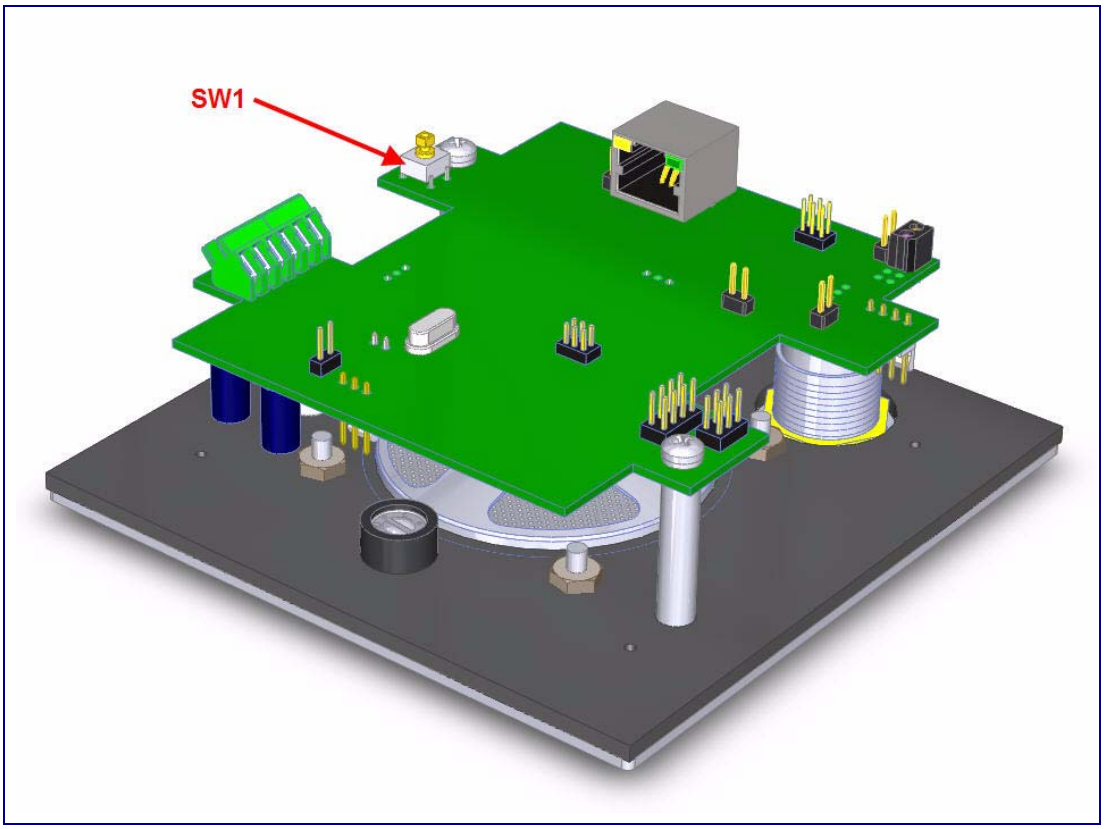
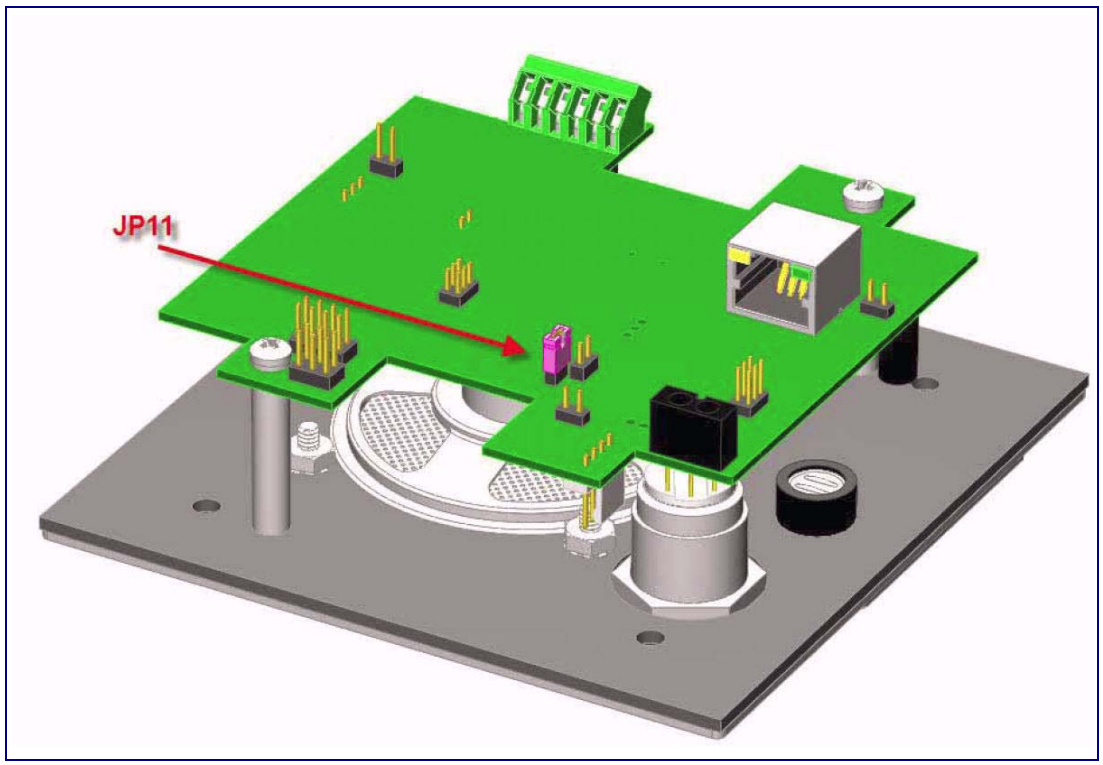


Figure 2-9. Jumper on JP11



2.1.7 Announcing the IP Address

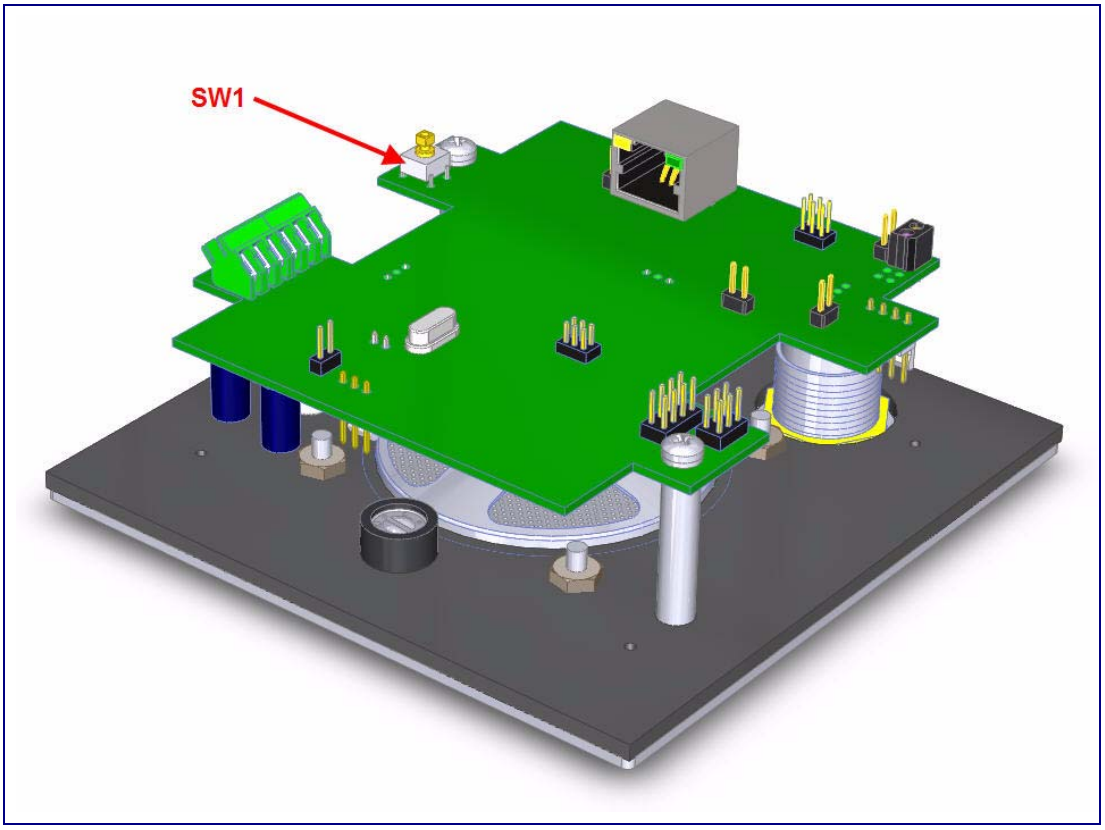
To announce a device's current IP address, first determine if you have an Intercom with an RTFM button (see **SW1** in Figure 2-10), and then do one of the following:

- If you have an Intercom that has an RTFM button, then see Section 2.1.7.1, "Intercom with an RTFM Button".
- If you have an Intercom that has a jumper and does not have an RTFM button, then see Section 2.1.7.2, "Intercom with a Jumper and No RTFM Button".

2.1.7.1 Intercom with an RTFM Button

1. If you have an Intercom with an RTFM button, then press and hold the RTFM button (see **SW1** in Figure 2-10) until the IP address is announced.
2. Release the Call Button after the IP address is announced.

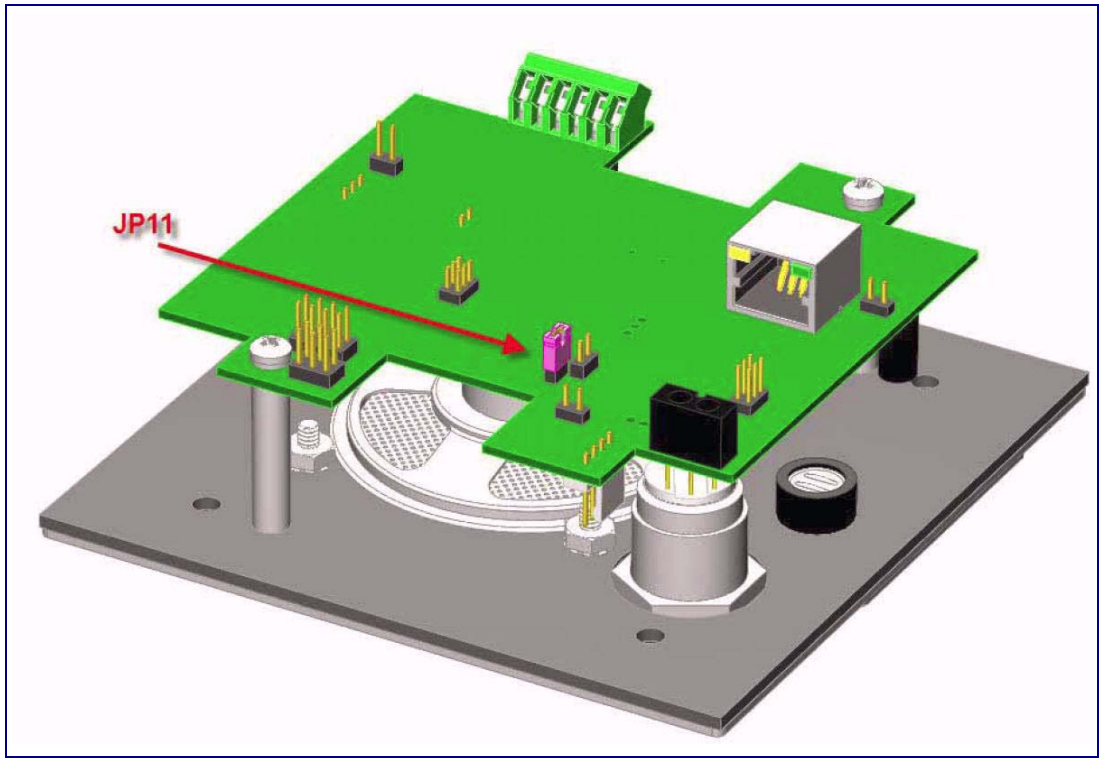
Figure 2-10. RTFM Button (SW1 Button)



2.1.7.2 Intercom with a Jumper and No RTFM Button

1. If you have an Intercom with a jumper and no RTFM button, then install a jumper on JP11. See **JP11** in Figure 2-11.
2. Wait until the IP address is announced.
3. Remove the jumper and restart the unit.

Figure 2-11. Jumper on JP11



2.1.8 Restore the Factory Default Settings

When troubleshooting configuration problems, it is sometimes convenient to restore the device to a known state. To restore the factory default settings on your device, do one of the following:

- If you have an Intercom that has an RTFM Button, then see Section 2.1.8.1, "Intercom with an RTFM Button".
- If you have an Intercom that has a jumper and does not have an RTFM button, then see Section 2.1.8.2, "Intercom with a Jumper".

Note Each Intercom is delivered with factory set default values.

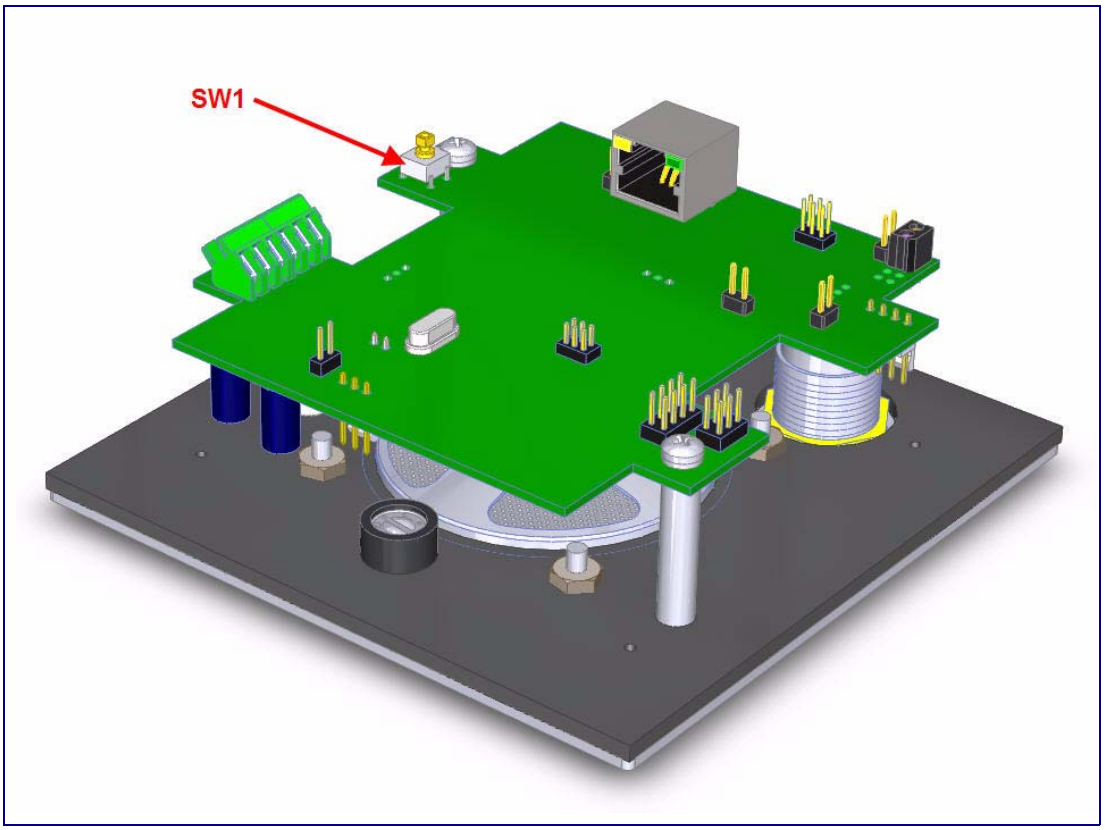
Note The device will use DHCP to obtain the new IP address (DHCP-assigned address or default to 10.10.10.10 if a DHCP server is not present).

2.1.8.1 Intercom with an RTFM Button

Complete the following steps to restore defaults on an Intercom that has an RTFM button:

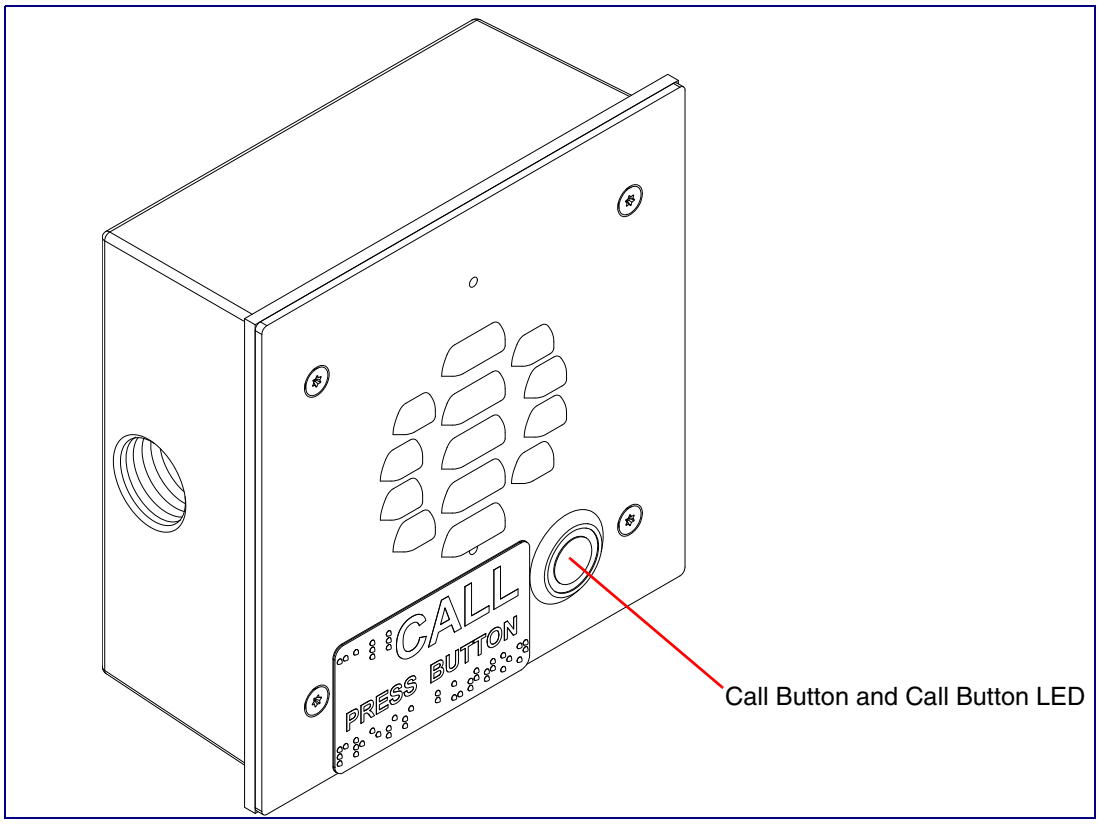
1. Press and hold the RTFM button (**SW1** in Figure 2-12) until the Intercom announces the IP address.

Figure 2-12. RTFM Button (SW1 Button)



2. The Call Button LED (see Figure 2-13) on the front will blink quickly.
3. Press and hold the Call Button until "*restoring defaults*" is announced.

Figure 2-13. Call Button and Call Button LED



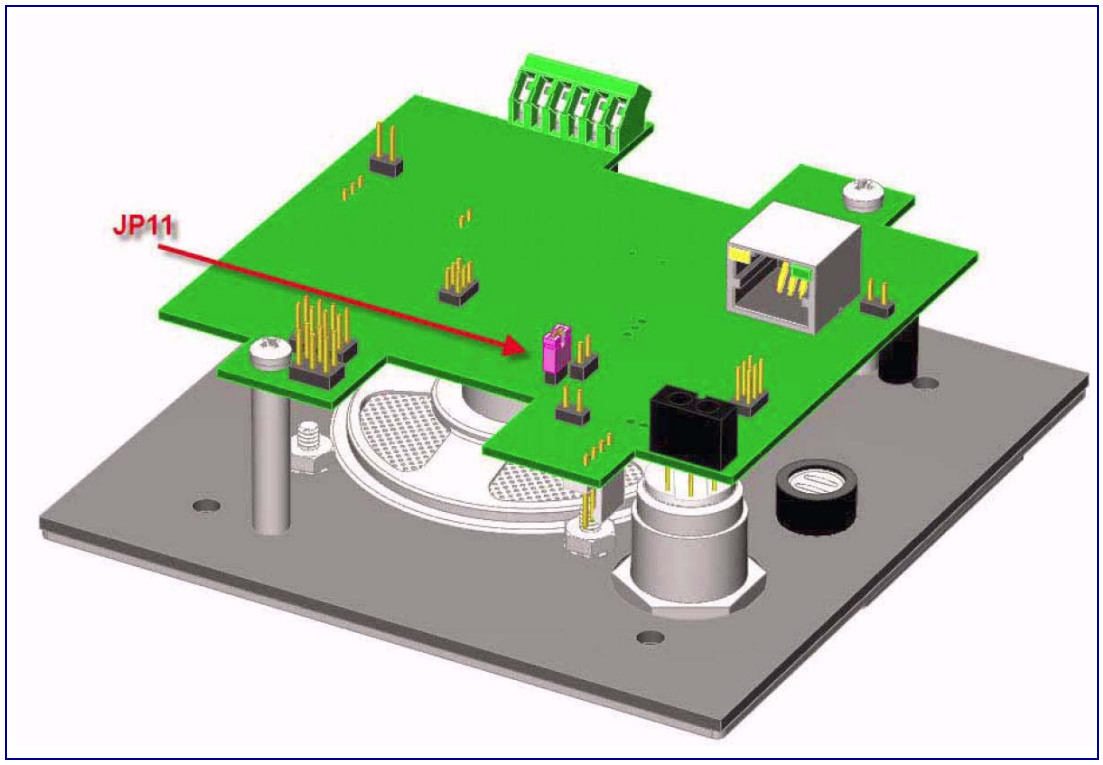
4. Release the Call Button and wait for the Intercom to reboot.

2.1.8.2 Intercom with a Jumper

Complete the following steps to restore defaults on an Intercom that has a jumper and no RTFM button:

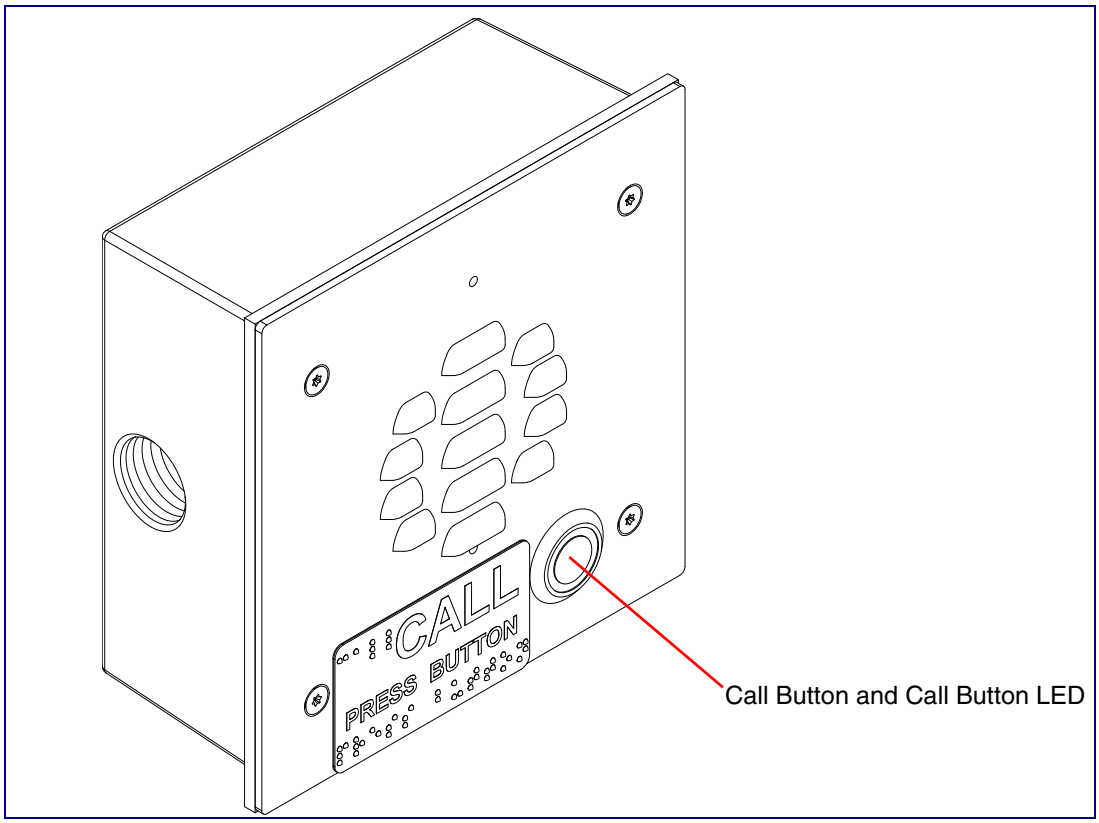
1. Put a jumper on JP11. See Figure 2-14.

Figure 2-14. Jumper on JP11



2. Wait for the Intercom to announce the IP address.
3. Press and hold the Call Button (see Figure 2-15) until "*restoring defaults*" is announced.
4. Release the Call Button and wait for the Intercom to reboot.
5. Remove the jumper and cycle power by unplugging Intercom and plugging it back in.

Figure 2-15. Call Button and Call Button LED



2.1.9 Adjust the Volume

You can adjust the volume through the Speaker Volume setting on the Device Configuration Page.

2.2 Configure the Intercom Parameters

To configure the Intercom online, use a standard web browser.

Configure each Intercom and verify its operation *before* you mount it. When you are ready to mount an Intercom, refer to Appendix A, "Mounting the Intercom" for instructions.

All Intercoms are initially configured with the following default IP settings:

When configuring more than one Intercom, attach the Intercoms to the network and configure one at a time to avoid IP address conflicts.

Table 2-4. Factory Default Settings

Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address[a]	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask[a]	255.0.0.0
Default Gateway[a]	10.0.0.1

a. Default if there is not a DHCP server present.

2.2.1 Intercom Web Page Navigation

Table 2-5 shows the navigation buttons that you will see on every Intercom web page.

Table 2-5. Web Page Navigation

Web Page Item	Description
	Link to the **Home** page.
	Link to the **Device Configuration** page.
	Link to the **Networking** page.
	Link to go to the **SIP Configuration** page.
	Link to go to the **Nightringer** page.
	Link to the **Sensor Configuration** page.
	Link to the **Multicast Configuration** page.
	Link to the **Audio Configuration** page.
	Link to the **Event Configuration** page.
	Link to the **Autoprovisioning Configuration** page.
	Link to the **Update Firmware** page.

2.2.2 Log in to the Configuration Home Page

1. Open your browser to the Intercom IP address.

Note If the network does not have access to a DHCP server, the device will default to an IP address of 10.10.10.10.

Note Make sure that the PC is on the same IP network as the Intercom.

Note You may also download CyberData's VoIP Discovery Utility program which allows you to easily find and configure the default web address of the CyberData VoIP products.

CyberData's VoIP Discovery Utility program is available at the following website address:

http://www.cyberdata.net/support/voip/discovery_utility.html

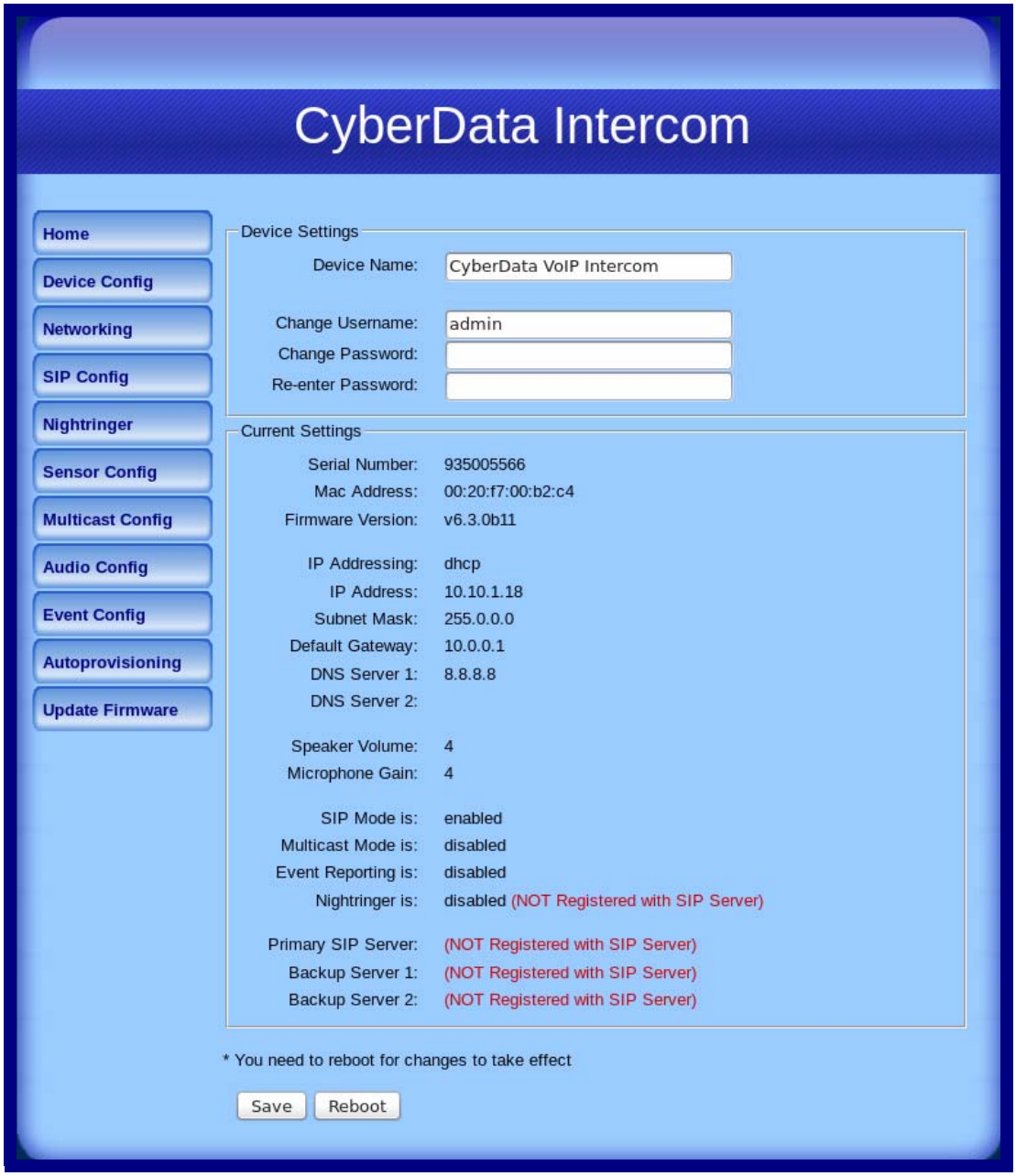
Note The Intercom ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

2. When prompted, use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 2-16):

   Web Access Username: **admin**

   Web Access Password: **admin**

Figure 2-16. Home Page



3. On the **Home Page**, review the setup details and navigation buttons described in Table 2-6.

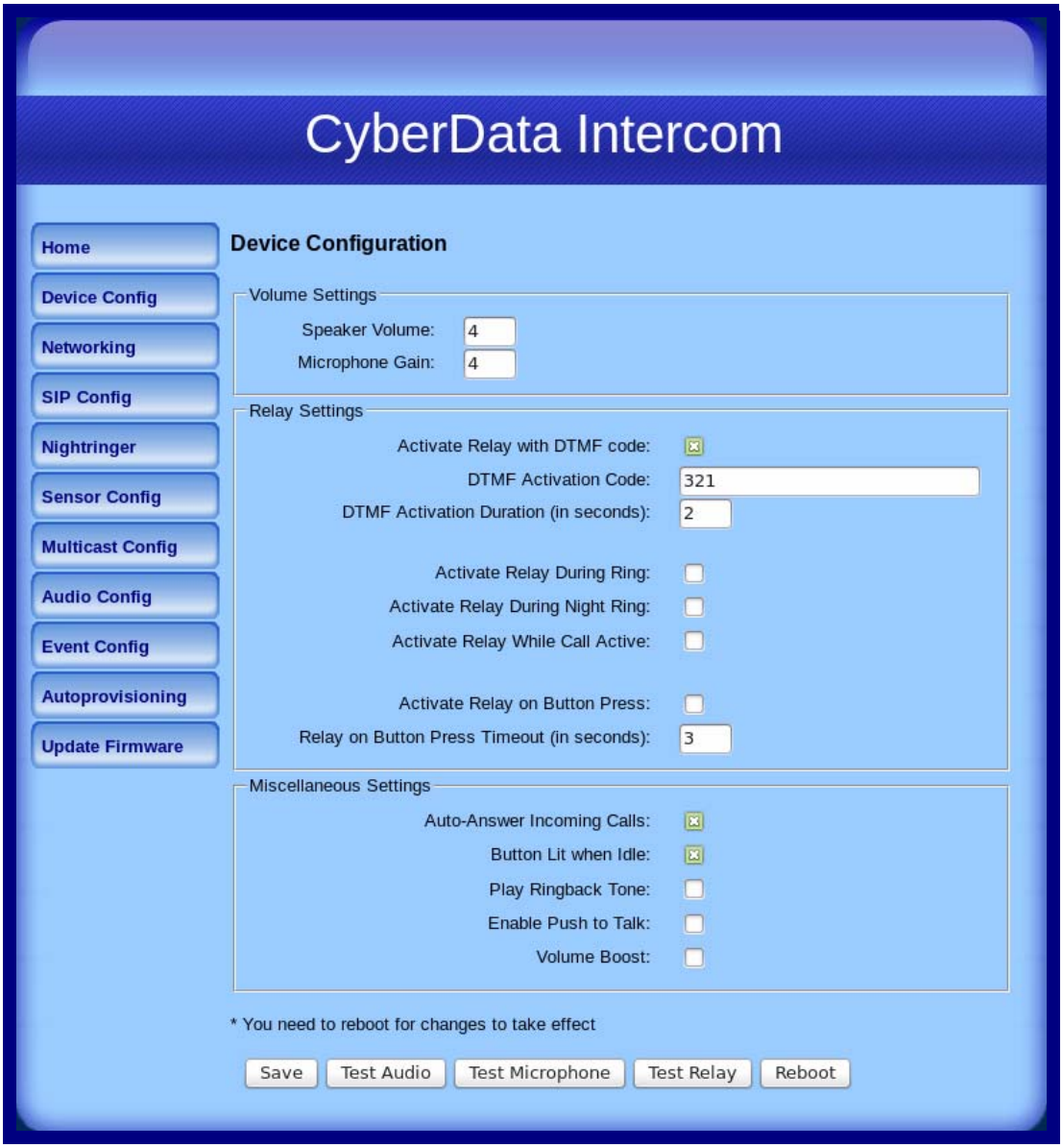
Table 2-6. Home Page Overview

Web Page Item	Description
Device Settings	
Device Name	Shows the device name.
Change Username	Type in this field to change the username.
Change Password	Type in this field to change the password.
Re-enter Password	Type the password again in this field to confirm the new password.
Current Settings	
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
IP Addressing	Shows the current IP addressing setting (**DHCP** or **static**).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
Speaker Volume	Shows the current speaker volume level.
Microphone Gain	Shows the current microphone gain level.
SIP Mode is	Shows the current status of the SIP mode.
Multicast Mode is	Shows the current status of the Multicast mode.
Event Reporting is	Shows the current status of the Event Reporting mode.
Nightringer is	Shows the current status of the Nightringer mode.
Primary SIP Server	Shows the current status of the Primary SIP Server.
Backup Server 1	Shows the current status of Backup Server 1.
Backup Server 2	Shows the current status of Backup Server 2.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

2.2.3 Configure the Device

1. Click the **Device Configuration** button to open the **Device Configuration** page. See Figure 2-17.

Figure 2-17. Device Configuration Page



2. On the **Device Configuration** page, you may enter values for the parameters indicated in Table 2-7.

Table 2-7. Device Configuration Parameters

Web Page Item	Description
Volume Settings	
Speaker Volume	Type the desired Intercom volume level into this field.
Microphone Gain	Type the desired microphone gain level into this field.
Relay Settings	
Activate Relay with DTMF Code	When selected, the relay can be activated with a DTMF code.
DTMF Activation Code	Type the desired DTMF activation code (25 character limit).
DTMF Activation Duration (in seconds)	Type the desired DTMF activation duration (in seconds) (2 character limit [activation times now go up to 99 seconds]). **NOTE**: A DTMF activation duration of **0** will toggle the relay indefinitely or until the activation code is sent again
Activate Relay During Ring	When selected, the relay will be activated for as long as the call is active. **NOTE**: When the phone is set to **Auto Answer**, it will not ring and this option does nothing.
Activate Relay During Night Ring	Check this box to activate the relay for as long as a Night Ring tone is ringing.
Activate Relay While Call Active	When selected, the relay will be activated for as long as the call is active.
Activate Relay on Button Press	When selected, the relay will be activated when the Call Button is pressed.
Relay on Button Press Timeout (in seconds)	Type the desired time (in seconds) that you want the relay to activate after the Call Button is pressed (1 character limit).
Miscellaneous Settings	
Auto-Answer Incoming Calls	When selected, the device will automatically answer incoming calls. When **Auto Answer** is Off, the device will play a ringtone through the Intercom speaker until someone presses the button.
Button Lit When Idle	When selected, the Call Button remains lit when idle.
Play Ringback Tone	When selected, you will hear a ringback tone while making a call.

Table 2-7. Device Configuration Parameters (continued)

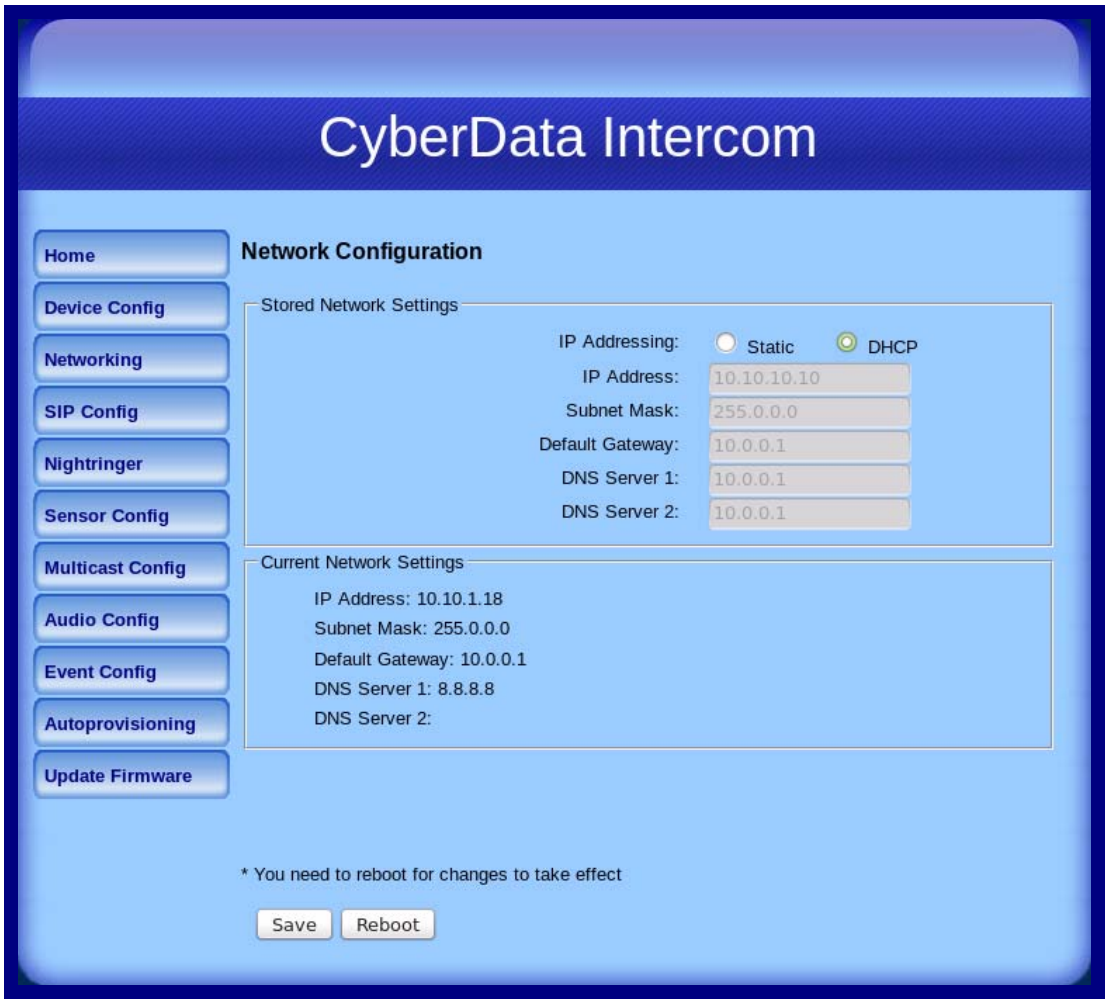
Web Page Item	Description
Enable Push to Talk	This option is for noisy environments. When enabled, the microphone will be muted normally. When the button is pressed and held, it will unmute the microphone and allow the operator to send audio back. **NOTE**: When **Enable Push to Talk** is enabled, you cannot stop an active call with the call button. The device on the other end will need to end the call. **NOTE**: **Enable Push to Talk** will not work on some older hardware.
Volume Boost	When **Volume Boost** is enabled, the device will play at a higher volume at the risk of having the audio clip at very high levels.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Test Audio	Click on the **Test Audio** button to do an audio test. When the **Test Audio** button is pressed, you will hear a voice message for testing the device audio quality and volume.
Test Relay	Click on the **Test Relay** button to do a relay test.
Test Microphone	Click on the **Test Microphone** button to do a microphone test. When the **Test Microphone** button is pressed, the following occurs: 1. The device will immediately start recording 3 seconds of audio. 2. The device will beep (indicating the end of recording). 3. The device will play back the recorded audio.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click the **Save** button.

2.2.4 Configure the Network Parameters

1. Click the **Networking** button to open the **Network Configuration** page (Figure 2-18).

Figure 2-18. Network Configuration Page



2. On the **Network Configuration** page, enter values for the parameters indicated in Table 2-8.

Table 2-8. Network Configuration Parameters

Web Page Item	Description
IP Addressing	Select either **DHCP IP Addressing** or **Static IP Addressing** by marking the appropriate radio button. If you select **Static**, configure the remaining parameters indicated in Table 2-8. If you select **DHCP**, go to Step 3.
Network Settings	
IP Address	Enter the Static IP address.
Subnet Mask	Enter the Subnet Mask address.
Default Gateway	Enter the Default Gateway address.
DNS Server 1	Enter the DNS Server 1 address.
DNS Server 2	Enter the DNS Server 2 address.
Current Network Settings	Shows the current network settings.
IP Address	Shows the current Static IP address.
Subnet Mask	Shows the current Subnet Mask address.
Default Gateway	Shows the current Default Gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click **Save Settings**. This updates the changed parameters and reboots the Intercom if appropriate.

4. Connect the Intercom to the target network.

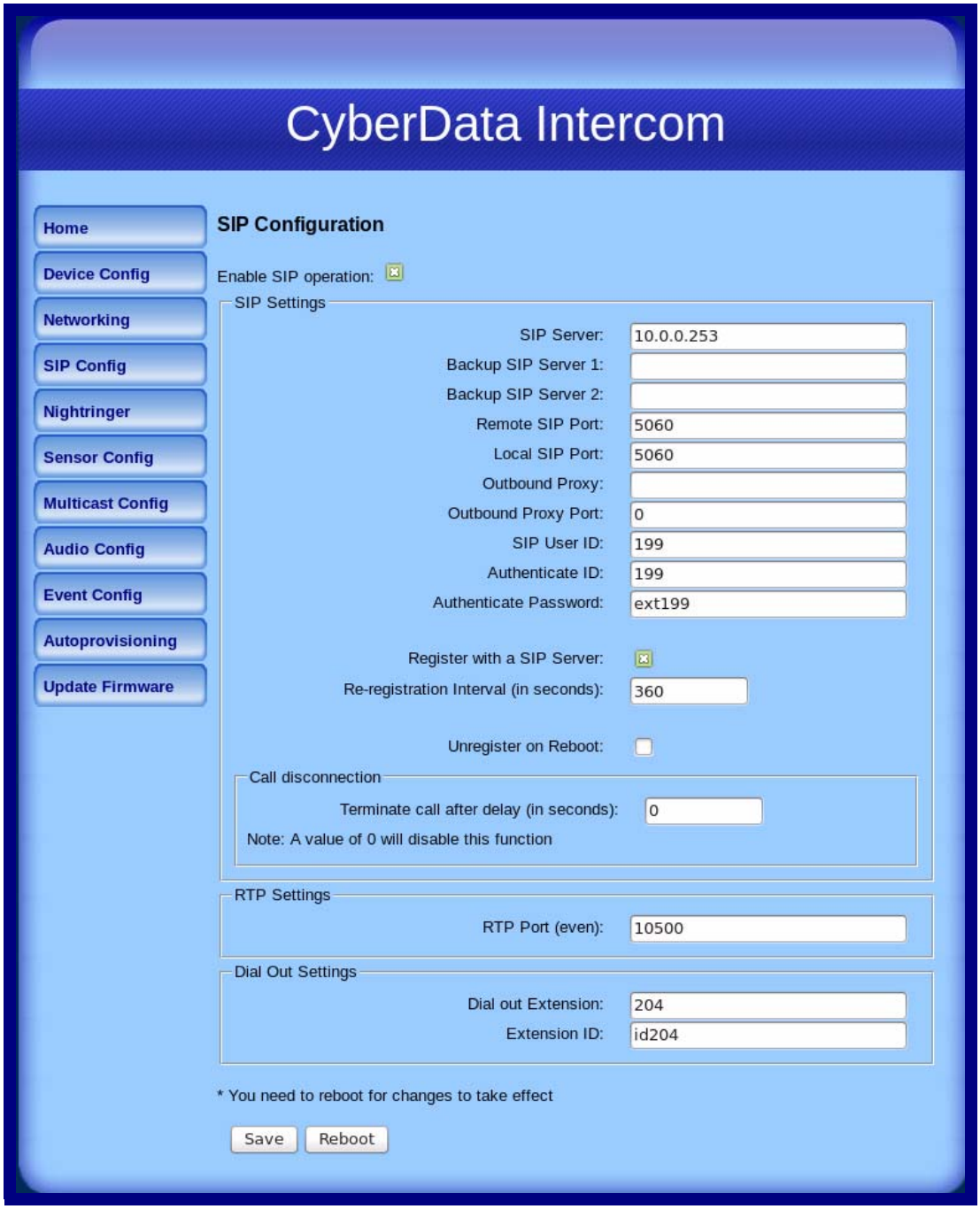
5. From a system on the same network as the Intercom, open a browser with the new IP address of the Intercom.

2.2.5 Configure the SIP Parameters

1. Click **SIP Config** to open the **SIP Configuration** page (Figure 2-19).

Note For specific server configurations, go to the following website address: http://www.cyberdata.net/support/server/index.html

Figure 2-19. SIP Configuration Page



2. On the **SIP Configuration** page, enter values for the parameters indicated in Table 2-9.

Table 2-9. SIP Configuration Parameters

Web Page Item	Description
Enable SIP Operation	Enables or disables SIP operation.
SIP Settings	
SIP Server	Use this field to set the address (in dotted decimal notation or as a canonical name) of the SIP registrar. This field can accept canonical names of up to 255 characters in length.
Backup SIP Server 1 Backup SIP Server 2	When the primary SIP Server goes offline and the device fails to register after the normal re-registration interval, the controller will fall back to using Backup SIP Server 1. If Backup SIP Server 1 fails, the device will use Backup SIP Server 2. If a higher priority SIP Server comes back online, the device will switch back to this server. You can leave the **Backup SIP Server 1** and **Backup SIP Server 2** fields blank.
Remote SIP Port*	Type the **Remote SIP Port** number (default 5060) (8 character limit).
Local SIP Port*	Type the **Local SIP Port** number (default 5060) (8 character limit).
Outbound Proxy	Type the Outbound Proxy as either a numeric IP address in dotted decimal notation or the fully qualified host name (255 character limit [FQDN]).
Outbound Proxy Port	Type the Outbound Proxy Port number (8 character limit).
SIP User ID*	Type the **SIP User ID** (up to 64 alphanumeric characters).
Authenticate ID*	Type the **Authenticate ID** (up to 64 alphanumeric characters).
Authenticate Password*	Type the **Authenticate Password** (up to 64 alphanumeric characters).
Register with a SIP Server*	Check this box to enable SIP Registration. For information about Point-to-Point Configuration, see Section 2.2.5.2, "Point-to-Point Configuration".
Re-registration Interval (in seconds)*	Type the SIP Registration lease time in minutes (default is 60 minutes) (8 character limit). Re-registration Interval (in seconds)*
Unregister on Reboot*	When selected, on boot, the device will first register with a SIP server with a expiration delay of 0 seconds. This has the effect of unregistering any current devices on this extension.

Table 2-9. SIP Configuration Parameters (continued)

Web Page Item	Description
Call Disconnection	
Terminate call after delay (in seconds)	Type the desired number of seconds that you want to transpire before a call is terminated. Note: A value of **0** will disable this function.
RTP Settings	
RTP Port (even)	Specify the port number used for the RTP stream after establishing a SIP call. This port number has to be an even number and defaults to 10500.
Dial Out Settings	
Dial Out Extension	Type the dial out extension number (64 character limit). **Note**: For information about dial-out extension strings and DTMF tones, see Section 2.2.5.1, "Dial Out Extension Strings and DTMF Tones (using rfc2833)".
Extension ID	Type the desired Extension ID (64 character limit).
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click **Save Settings**.

2.2.5.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

On the **SIP Configuration Page**, dial out extensions support the addition of comma delimited pauses and sending additional DTMF tones (using rfc2833). The first comma will pause three seconds after a call is first established with a remote device. Subsequent commas will pause for 2 seconds. A pause of one second will be sent after each numerical digit.

Table 2-10. Examples of Dial-Out Extension Strings

Extension String	Resulting Action
302	Dial out extension 302 and establish a call
302,2	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2'
302,25,,,4,,1	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2', send out DTMF tone 5, wait 6 seconds, send out DTMF tone 4, wait 4 seconds, send out DTMF tone 1

Note The maximum number of total characters in the dial-out field is 64.

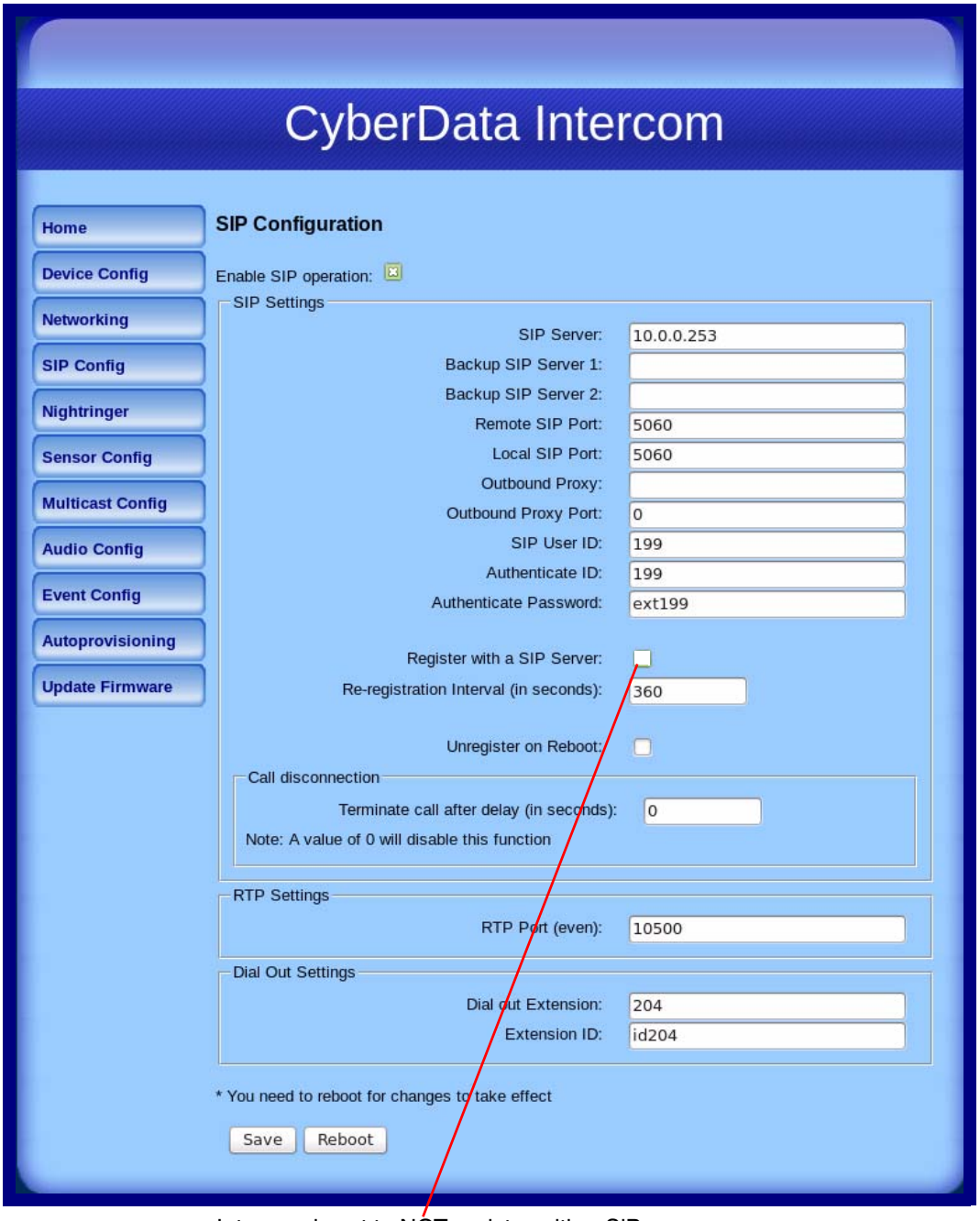
2.2.5.2 Point-to-Point Configuration

When the board is set to not register with a SIP server (see Figure 2-20), it's possible to set the intercom to dial out to a single endpoint.

In this case, the dial-out extension should be the IP address of the remote device. The Intercom can also receive Point-to-Point calls. The delayed DTMF functionality is available in the Point-to-Point Mode.

Note Receiving point-to-point SiP calls may not work with all phones.

Figure 2-20. SIP Configuration Page Set to Point-to-Point Mode



2.2.5.3 Delayed DTMF

On the **SIP Configuration** page the dial out extension supports the addition of comma delimited pauses and sending additional DTMF tones (using rfc2833). The first comma will pause three seconds after a call is first established with a remote device. Subsequent commas will pause for 2 seconds. A pause of one second will be sent after each numerical digit.

Table 2-11. Examples of Dial-Out Extension Strings

Extension String	Resulting Action
302	Dial out extension 302 and establish a call
302,2	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2'
302,25,,,4,,1	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2', send out DTMF tone 5, wait 6 seconds, send out DTMF tone 4, wait 4 seconds, send out DTMF tone 1

Note The maximum number of total characters in the dial-out field is 25.

2.2.6 Configure the Nightringer Parameters

When the Nightringer is enabled, the Intercom will register as a second SIP extension. Registration does not have to be to the same server as the primary SIP registration. Any calls made to the Nightringer extension will cause the Intercom to play a ring tone. There is no way to answer this call. The Nightringer is designed to be used in buildings where calls made after hours are directed to a ring group.

1. Click on the **Nightringer** button to open the **Nightringer Configuration** page. See Figure 2-21.

Figure 2-21. Nightringer Configuration Setup

2. On the **Nightringer Configuration** page, enter values for the parameters indicated in Table 2-12.

Table 2-12. Nightringer Configuration Parameters

Web Page Item	Description
Enable Nightringer	When the nightringer is enabled, the unit will attempt to register a second extension with the SIP server. Any calls made to this extension will play a ringtone.
Nightringer Settings	
SIP Server	Type the SIP server represented as either a numeric IP address in dotted decimal notation.
Remote SIP Port	Type the Remote SIP Port number (default 5060) (8 character limit).
Local SIP Port	Type the Local SIP Port number (default 5060) (8 character limit). **Note**: This value cannot be the same as the **Local SIP Port*** found on the **SIP Configuration Page**.
User ID	Type the **User ID** (up to 64 alphanumeric characters).
Authenticate ID	Type the **Authenticate ID** (up to 64 alphanumeric characters).
Authenticate Password	Type the **Authenticate Password** (up to 64 alphanumeric characters).
Re-registration Interval (in seconds)*	Type the SIP Registration lease time in minutes (default is 60 minutes) (8 character limit). Re-registration Interval (in seconds)*
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click on the **Save** button.

2.2.7 Configure the Sensor Configuration Parameters

The door sensor (pins 5 and 6) on the header can be used to monitor a door's open or closed state. There is an option on the **Sensor Configuration** page to trigger on an open or short condition on these pins. The door sensor alarm will be activated when the **Door Open Timeout** parameter has been met.

The intrusion sensor is an optical sensor installed on the Intercom board and will be activated when the Intercom is removed from the case.

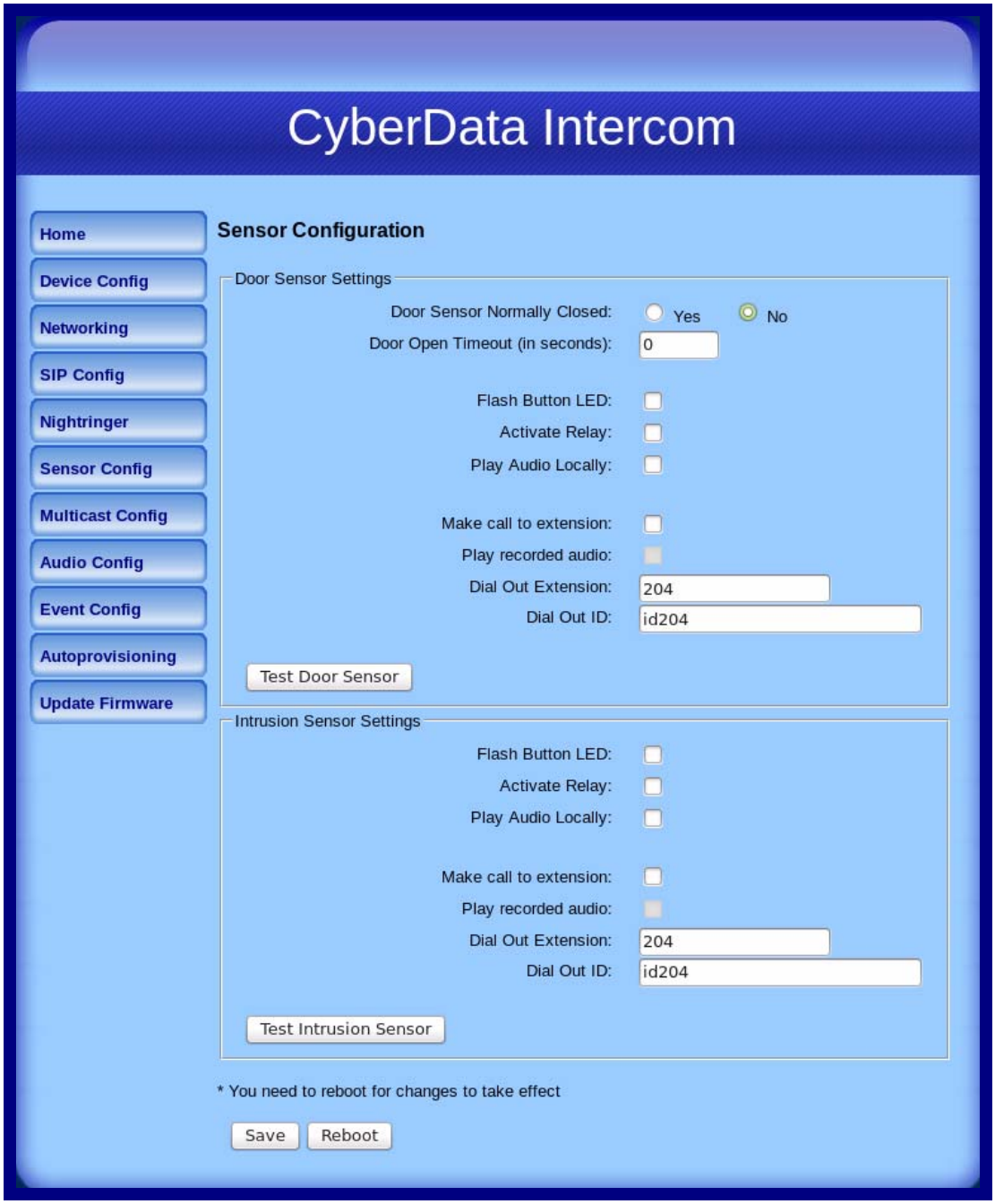
For each sensor there are four actions the Intercom can take:

- Flash the LED until the sensor is deactivated (roughly 10 times/second)
- Activate the relay until the sensor is deactivated
- Loop an audio file out of the Intercom speaker until the sensor is deactivated
- Call a preset extension and play a pre-recorded audio file (once)

Note Calling a preset extension can be set up as a point-to-point call, but currently can't send delayed DTMF tones.

1. Click **Sensor Config** to open the **Sensor Configuration** page (Figure 2-22).

Figure 2-22. Sensor Configuration Page



2. On the **Sensor Configuration** page, enter values for the parameters indicated in Table 2-13.

Table 2-13. Sensor Configuration Parameters

Web Page Item	Description
Door Sensor Settings	
Door Sensor Normally Closed	Select the inactive state of the door sensors.
Door Open Timeout (in seconds)	Select the number of seconds that you want to pass before the door sensor is activated.
Flash Button LED*	Check this box to flash the LED until the sensor is deactivated (roughly 10 times/second).
Activate Relay	Check this box to activate the relay until the sensor is deactivated.
Play Audio Locally	Check this box to loop an audio file out of the Intercom speaker until the sensor is deactivated.
Make call to extension	Check this box to call a preset extension (once).
Play recorded audio	Check this box to play a pre-recorded audio file (once).
Dial Out Extension	Enter the desired dial-out extension number.
Extension ID	Type the desired Extension ID (64 character limit).
Test Door Sensor	Use this button to test the door sensor.
Intrusion Sensor Settings	
Flash Button LED*	Check this box to flash the LED until the sensor is deactivated (roughly 10 times/second).
Activate Relay	Check this box to activate the relay until the sensor is deactivated.
Play Audio Locally	Check this box to loop an audio file out of the Intercom speaker until the sensor is deactivated.
Make call to extension	Check this box to call a preset extension (once).
Play recorded audio	Check this box to play a pre-recorded audio file (once).
Dial Out Extension	Enter the desired dial-out extension number.
Extension ID	Type the desired Extension ID (64 character limit).
Test Intrusion Sensor	Use this button to test the Intrusion sensor.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click **Save Settings**.

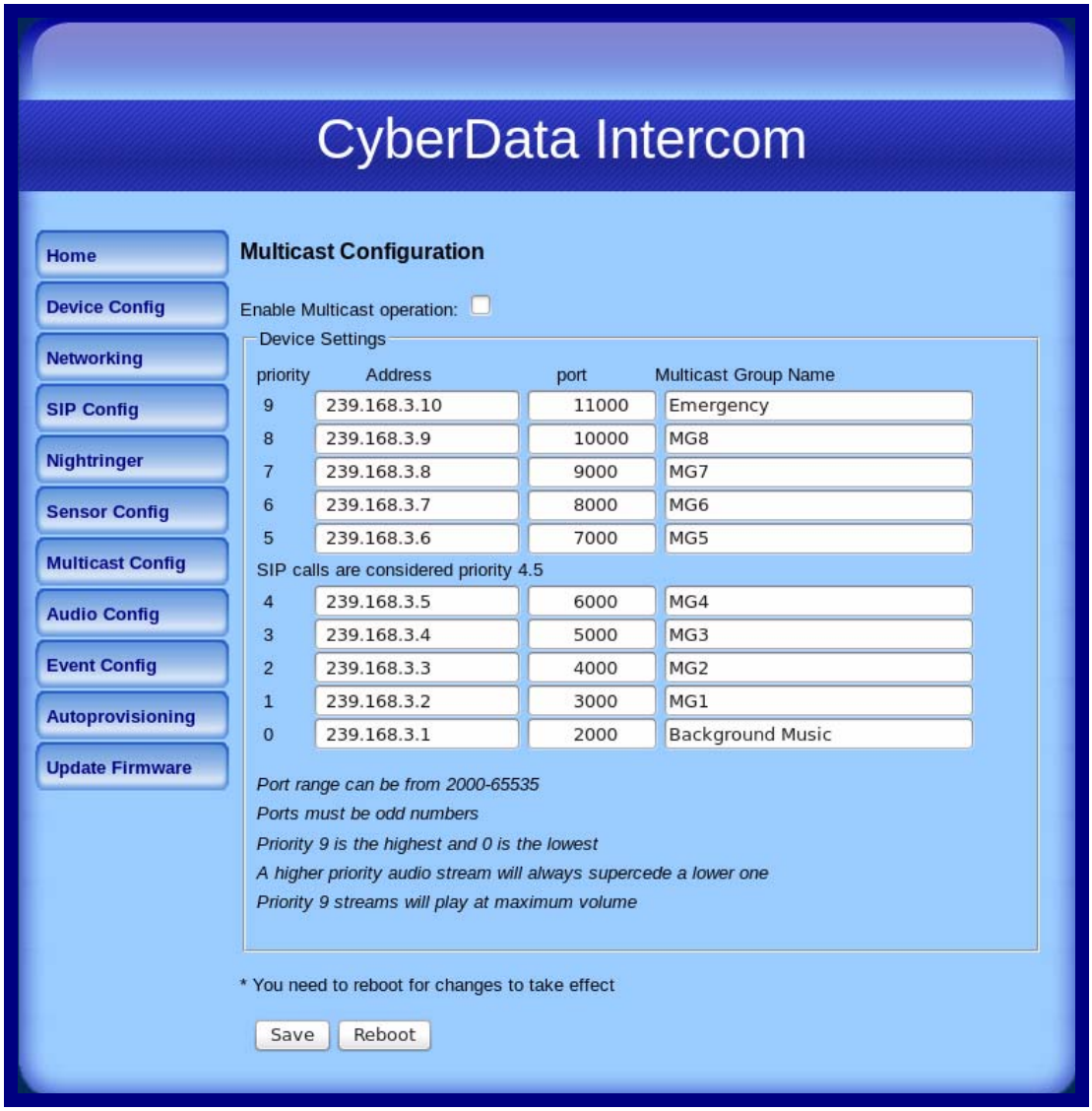
2.2.8 Configure the Multicast Parameters

Multicast groups use multicasting to create public address paging zones. Multicasting is based on the concept of a group. Multicast addresses specify an arbitrary group of IP hosts that have joined the group and want to receive traffic sent to the group. Group members send IGMP messages to their local multicast routers, allowing the group traffic traversal from the source.

The **Multicast Configuration** page allows the Intercom to join up to 10 paging zones for receiving ulaw/alaw encoded RTP audio streams. A paging zone can consist of one or many CyberData multicast group-enabled products. There is no limit to how many devices can be in a given paging zone. Each multicast group is defined by a multicast address and port number. Each multicast group is assigned a priority, allowing simultaneously arriving pages to be serviced based on importance. Multicast groups are compatible with IGMP through version three. The Intercom supports simultaneous SIP and Multicast.

1. Click on the **Multicast Configuration** button to open the **Multicast Configuration** page. See Figure 2-23.

Figure 2-23. Multicast Configuration Page



2. On the **Multicast Configuration** page, enter values for the parameters indicated in Table 2-14.

Table 2-14. Multicast Configuration Parameters

Web Page Item	Description
Enable Multicast Operation	Enables or disables multicast operation.
Device Settings	
Priority	Indicates the priority for the multicast group. Priority **9** is the highest (emergency streams). **0** is the lowest (background music). SIP calls are considered priority **4.5**. See Section 2.2.8.1, "Assigning Priority" for more details.
Address	Enter the multicast IP Address for this multicast group (15 character limit).
Port (range can be from 2000 to 65535)	Enter the port number for this multicast group (5 character limit). **Note**: The multicast ports have to be even values. The webpage will enforce this restriction.
Multicast Group Name	Assign a descriptive name for this multicast group (25 character limit).
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click on the **Save** button.

2.2.8.1 Assigning Priority

When playing multicast streams, audio on different streams will preempt each other according to their priority in the list. An audio stream with a higher priority will interrupt a stream with a lower priority.

If both SIP and Multicast is enabled, SIP audio streams are considered priority **4.5**. SIP audio will interrupt multicast streams with priority **0** through **4** and will be interrupted by multicast streams with priority **5** through **9**.

During priority **9** multicast streams, the analog volume control is bypassed and the volume level is set to maximum.

Note SIP calls, multicast streams, ring tones, ringback tones, and nightring tones are all prioritized.

Ringtones and Nightringtones

Ringtones all play at the same priority level. This means that it is possible to have a nightring tone and a normal ringtone playing at the same time.

2.2.9 Configure the Audio Configuration Parameters

The **Audio Configuration** page is used to add custom audio to the board. User uploaded audio will take precedence over the audio files shipped with the Intercom.

1. Click **Audio Config** to open the **Audio Configuration** page (Figure 2-24).

Figure 2-24. Audio Configuration Page

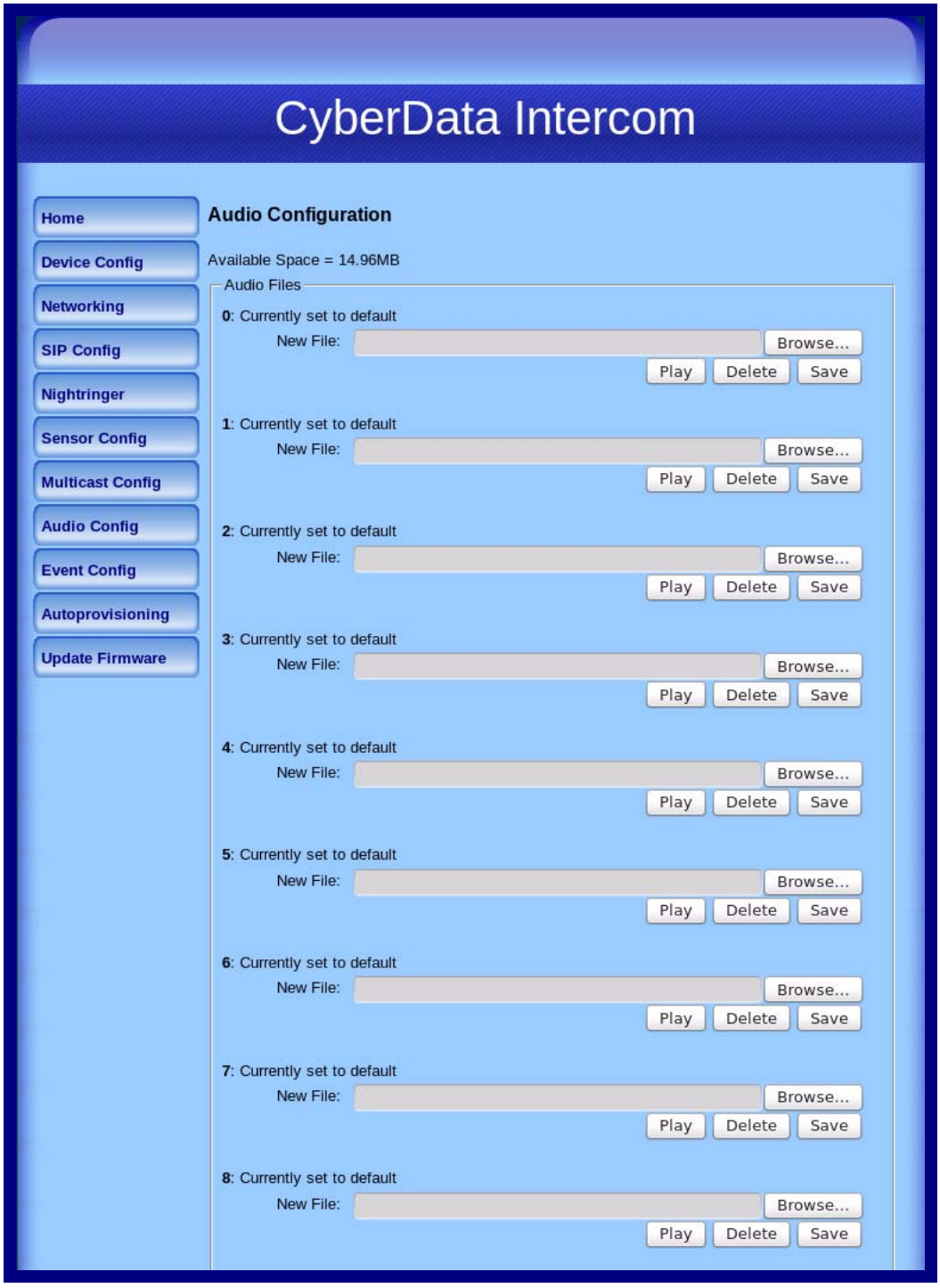


Figure 2-25. Audio Configuration Page (continued)

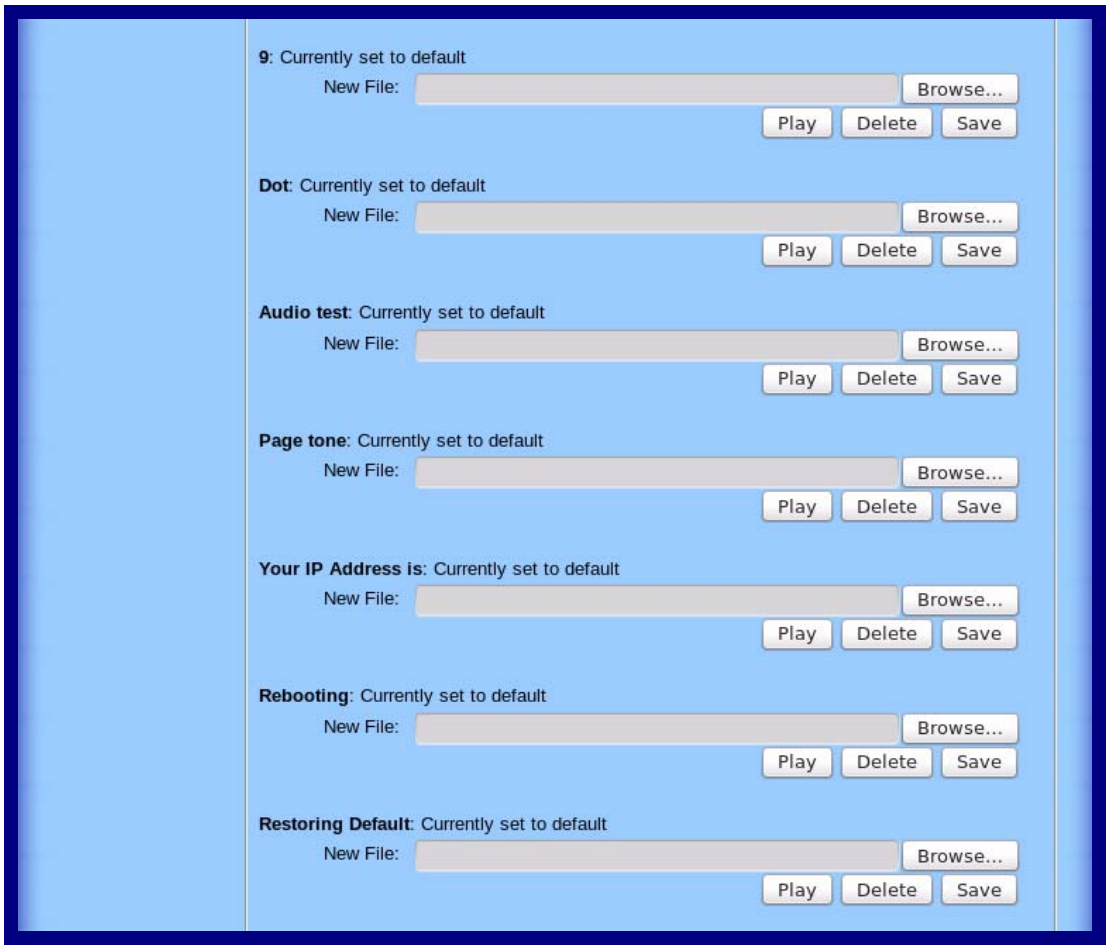
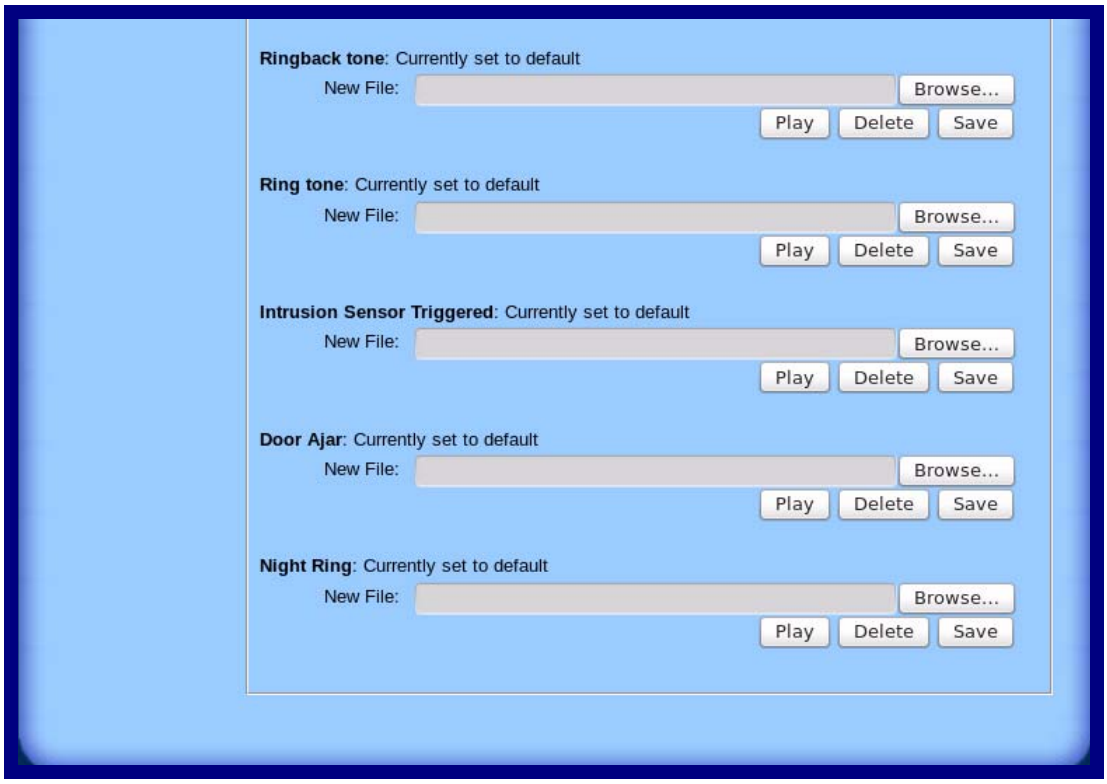


Figure 2-26. Audio Configuration Page (continued)



2. On the **Audio Configuration** page, enter values for the parameters indicated in Table 2-15.

Table 2-15. Audio Configuration Parameters

Web Page Item	Description
Audio Files	
0-9	The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit). '0' corresponds to the spoken word “zero.” '1' corresponds to the spoken word “one.” '2' corresponds to the spoken word “two.” '3' corresponds to the spoken word “three.” '4' corresponds to the spoken word “four.” '5' corresponds to the spoken word “five.” '6' corresponds to the spoken word “six.” '7' corresponds to the spoken word “seven.” '8' corresponds to the spoken word “eight.” '9' corresponds to the spoken word “nine.”
Dot	Corresponds to the spoken word “dot.” (24 character limit)
Audiotest	Corresponds to the message ***“This is the CyberData IP speaker test message...”*** (24 character limit)
Pagetone	Corresponds to a simple tone used for beep on initialization and beep on page (24 character limit).
Your IP Address is	Corresponds to the message “Your IP address is...” (24 character limit).
Rebooting	Corresponds to the spoken word “Rebooting” (24 character limit).
Restoring default	Corresponds to the message “Restoring default” (24 character limit).
Ringback Tone	This is the ringback tone that plays when calling a remote extension (24 character limit).
Ring Tone	This is the tone that plays when set to ring when receiving a call (24 character limit).
Intrusion Sensor Triggered	Corresponds to the message “Intrusion Sensor Triggered” (24 character limit).
Door Ajar	Corresponds to the message “Door Ajar” (24 character limit).
Night Ring	Specifies the ringtone for nightring. By default this parameter uses the same audio file that is selected for the **Ring Tone** parameter.
	The **Browse** button will allow you to navigate to and select an audio file.
	The **Play** button will play that audio file.
	The **Delete** button will delete any user uploaded audio and restore the stock audio file.

Table 2-15. Audio Configuration Parameters (continued)

Web Page Item	Description
	The **Save** button will download a new user audio file to the board once you've selected the file by using the **Browse** button. The **Save** button will delete any pre-existing user-uploaded audio files.

2.2.9.1 User-created Audio Files

User created audio files should be saved in the following format:

RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, mono 8000 Hz

You can use the free utility *Audacity* to convert audio files into this format. See Figure 2-27 through Figure 2-29.

Figure 2-27. Audacity 1

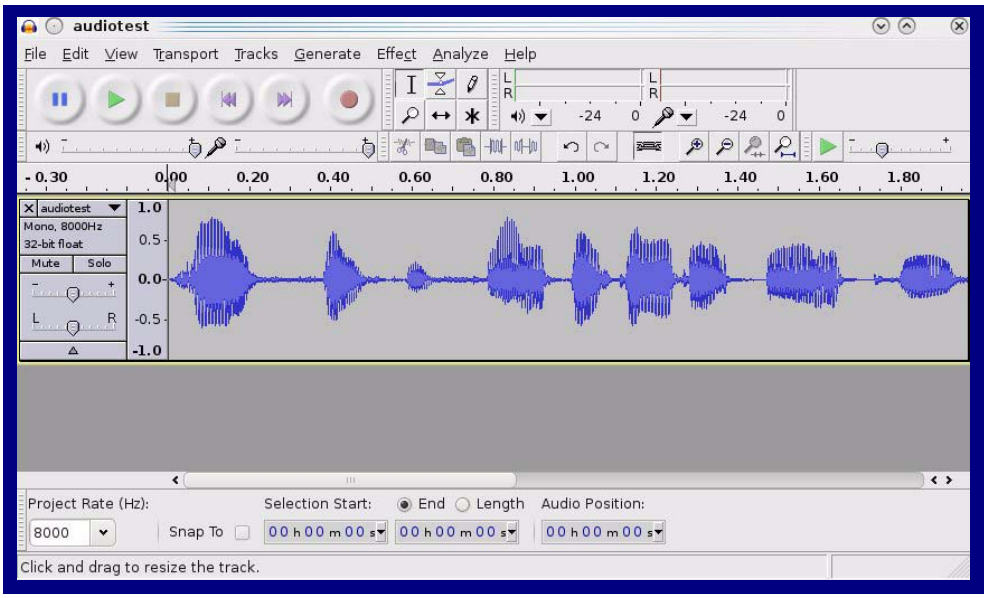
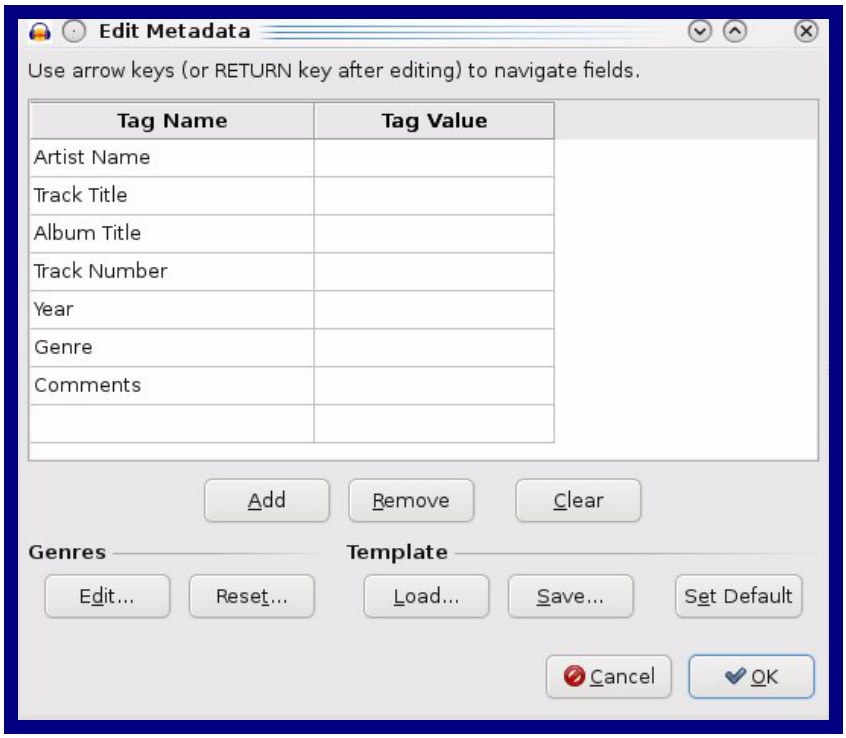


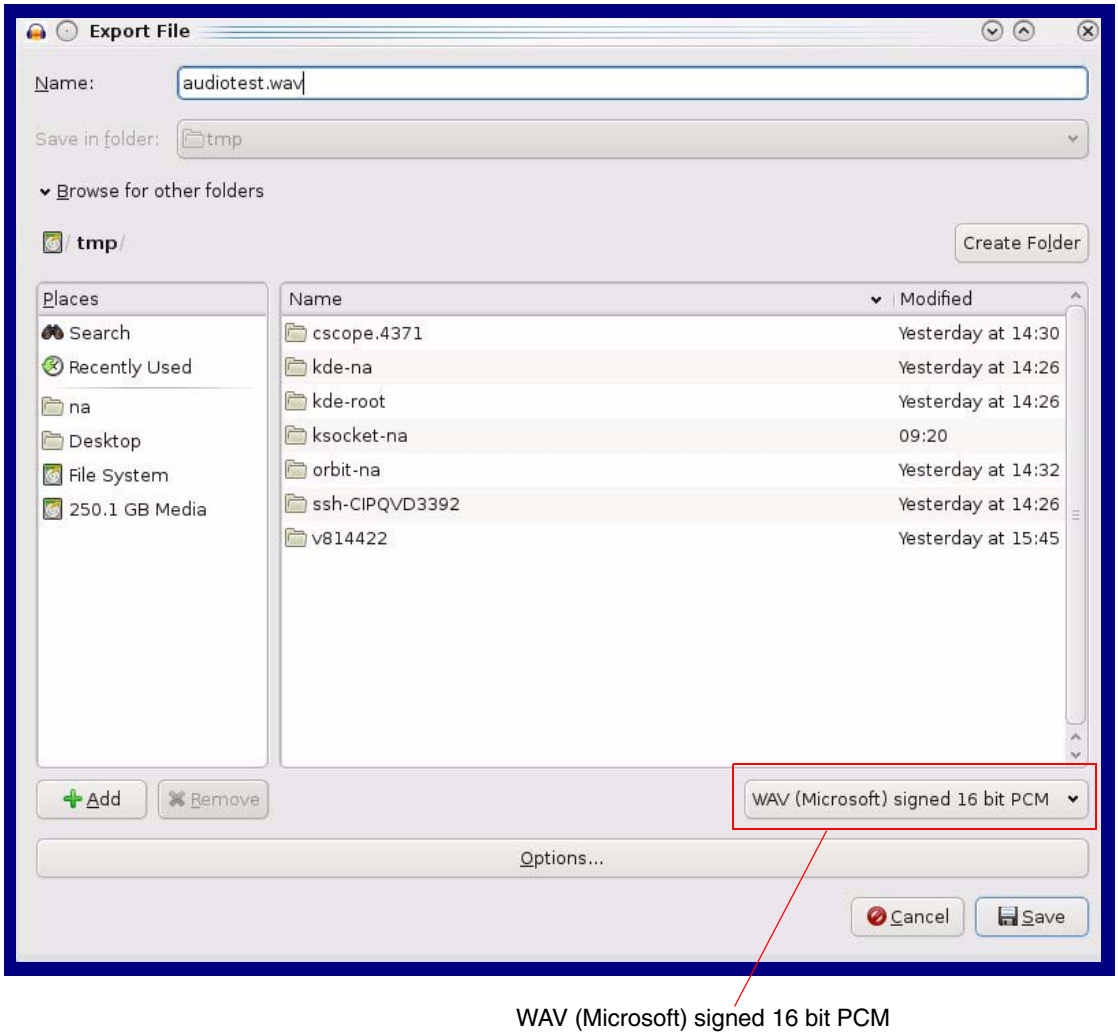
Figure 2-28. Audacity 2



When you export an audio file with Audacity, save the output as:

- **WAV (Microsoft) signed 16 bit PCM**.

Figure 2-29. WAV (Microsoft) signed 16 bit PCM



2.2.10 Configure the Event Parameters

Click the **Event Config** button to open the **Event Configuration** page (Figure 2-30). The **Event Configuration** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

Figure 2-30. Event Configuration Page

Table 2-16 shows the web page items on the **Event Configuration** page.

Table 2-16. Event Configuration

Web Page Item	Description
Enable Event Generation	When selected, Event Generation is enabled.
Remote Event Server	
Remote Event Server IP	Type the Remote Event Server IP address. (64 character limit)
Remote Event Server Port	Type the Remote Event Server port number. (8 character limit)
Remote Event Server URL	Type the Remote Event Server URL. (127 character limit)
Events	
Enable Button Events	When selected, Button Events are enabled.
Enable Call Active Events	When selected, Call Active Events are enabled.
Enable Call Terminated Events	When selected, Call Terminated Events are enabled.
Enable Relay Activated Events	When selected, Relay Activated Events are enabled.
Enable Relay Deactivated Events	When selected, Relay Deactivated Events are enabled.
Enable Ring Events	When selected, Ring Events are enabled.
Enable Night Ring Events	When selected, there is a notification when the unit receives a night ring.
Enable Multicast Start Events	When selected, Multicast Start Events are enabled.
Enable Multicast Stop Events	When selected, Multicast Stop Events are enabled.
Enable Power On Events	When selected, Power On Events are enabled.
Enable Sensor Events	When selected, Sensor Events are enabled.
Enable Intrusion Sensor Events	When selected, Intrusion Sensor Events are enabled.
Enable 60 Second Heartbeat Events	When selected, 60 Second Heartbeat Events are enabled.
	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
	Click on the **Test Event** button to test an event.
	Click on the **Reboot** button to reboot the system.

2.2.10.1 Example Packets for Events

The server and port are used to point to the listening server and the 'Remote Event Server URL' is the destination URL (typically the script running on the remote server that's used to parse and process the POST events).

Note The XML is URL-encoded before transmission so the following examples are not completely accurate.

Here are example packets for every event:

```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>POWERON</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 199
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>HEARTBEAT</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 196
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>BUTTON</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 201
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>CALL_ACTIVE</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
```

```
User-Agent: CyberData/1.0.0
Content-Length: 205
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>CALL_TERMINATED</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RINGING</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>MULTICAST_START</event>
<index>8</index>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 233
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>MULTICAST_STOP</event>
<index>8</index>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RELAY_ACTIVATED</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
```

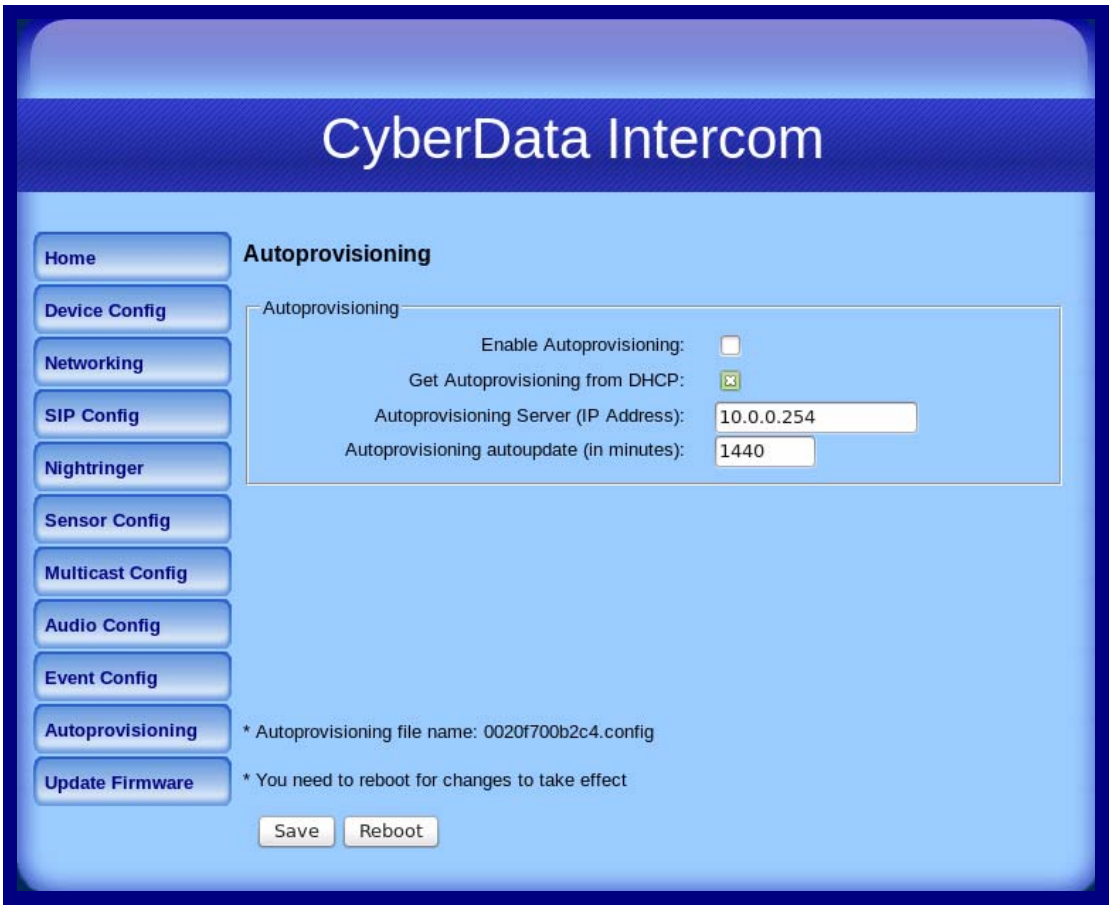
```
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RELAY_DEACTIVATED</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>NIGHTRINGING</event>
</cyberdata>
```

2.2.11 Configure the Autoprovisioning Parameters

1. Click the **Autoprovisioning** button to open the **Autoprovisioning Configuration** page. See Figure 2-31.

Figure 2-31. Autoprovisioning Configuration Page



2. On the **Autoprovisioning Configuration** page, you may enter values for the parameters indicated in Table 2-17.

Table 2-17. Autoprovisioning Configuration Parameters

Web Page Item	Description
Autoprovisioning	
Enable Autoprovisioning	See Section 2.2.11.1, "Autoprovisioning".
Get Autoprovisioning from DHCP	See Section 2.2.11.1, "Autoprovisioning".
Autoprovisioning Server (IP Address)	See Section 2.2.11.1, "Autoprovisioning" (15 character limit).
Autoprovisioning Autoupdate (in minutes)	Type the desired time (in minutes) that you want the Autoprovisioning feature to update (6 character limit).
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click the **Save** button.

2.2.11.1 Autoprovisioning

Enable Autoprovisioning Option

With autoprovisioning enabled, the board will get its configuration from a remote TFTP server on startup or periodically on a scheduled delay. Autoprovisioned values will override values stored in on-board memory and will be visible on the web page. The board gets its autoprovisioning information from an XML-formatted file hosted from a TFTP server. CyberData will provide a template for this XML file and the user can modify it for their own use.

To use autoprovisioning, create a copy of the autoprovisioning template with the desired settings and name this file with the mac address of the device to configure (for example: **0020f7350058.config**). Put this file into your TFTP server directory and manually set the TFTP server address on the board.

It is not necessary to set every option found in the autoprovisioning template. As long as the XML is valid, the file can contain any subset. Options not autoprovisioned will default to the values stored in the on board memory. For example if you only wanted to modify the device name, the following would be a valid autoprovisioning file:

```
<?xml version="1.0" encoding="utf-8" ?>
<specific>
    <MiscSettings>
        <DeviceName>auto Intercom</DeviceName>
    </MiscSettings>

</specific>
```

Networking

The board will only apply networking settings or firmware upgrades after a reboot.

Get Autoprovisioning from DHCP

When this option is checked, the device will automatically fetch its autoprovisioning server address from the DHCP server. The device will use the address specified in **OPTION 150** (TFTP-server-name) or **OPTION 66**. If both options are set, the device will use **OPTION 150**.

Refer to the documentation of your DHCP server for setting up **OPTION 150**.

To set up a Linux DHCPD server to serve autoprovisioning information (in this case using both option 66 and 150), here's an example dhcpd.conf:

```
# dhcpd.conf
#
# Configuration file for ISC dhcpd (see 'man dhcpd.conf')
#
ddns-update-style ad-hoc;

option option-150 code 150 = ip-address;

subnet 10.0.0.0 netmask 255.0.0.0 {
        max-lease-time 120;
        default-lease-time 120;

        option routers                  10.0.0.1;
        option subnet-mask              255.0.0.0;

        option domain-name              "voiplab";
        option domain-name-servers       10.0.0.1;

        option time-offset              -8;     # Pacific Standard Time

        option tftp-server-name         "10.0.0.254";

        option option-150               10.0.0.254;

        range 10.10.0.1 10.10.2.1;}
```

Autoprovisioning Server (IP Address)

Instead of using DHCP to provide the autoprovisioning tftp server address, you can specify an address manually.

Autoprovisioning Autoupdate

If **Autoprovisioning** is enabled and the **Autoprovisioning Autoupdate** value is something other than **0** minutes, a service is started on startup that will wait the configured number of minutes and then try to re-download its autoprovisioning file. It will compare its previously autoprovisioned file with this new file and if there are differences, it will reboot the board.

Autoprovisioned Firmware Upgrades

An Autoprovisioned firmware upgrade only happens after a reboot, will take roughly three minutes, and the web page will be unresponsive during this time.

The '**FirmwareVersion'** value in the xml file *must* match the version stored in the '**FirmwareFile**'.

```
<FirmwareVersion>v6.3.0</FirmwareVersion>
<FirmwareFile>630-intercom-uImage</FirmwareFile>
```

If these values are mismatched, the board can get stuck in a loop where it goes through the following sequence of actions:

1. The board downloads and writes a new firmware file.
2. After the next reboot, the board recognizes that the firmware version does not match.
3. The board downloads and writes the firmware file again.

CyberData has timed a firmware upgrade at 140 seconds. Therefore, if you suspect the board is stuck in a loop, either remove or comment out the **FirmwareVersion** line in the XML file and let the board boot as it normally does.

Autoprovisioned Audio Files

Audio files are stored in non-volatile memory and an autoprovisioned audio file will only have to be downloaded once for each device. Loading many audio files to the device from the web page could cause it to appear unresponsive. If this happens, wait until the transfer is complete and then refresh the page.

The device uses the file name to determine when to download a new audio file. This means that if you used autoprovisioning to upload a file and then changed the contents of this file at the TFTP server, the device will not recognize that the file has changed (because the file name is the same).

Since audio files are stored in non-volatile memory, if autoprovisioning is disabled after they have been loaded to the board, the audio file settings will not change. You can force a change to the audio files on the board by clicking **Restore Default** on the **Audio Configuration** page or by changing the autoprovisioning file with "**default**" set as the file name.

2.3 Upgrade the Firmware and Reboot the Intercom

Note To guard against failed firmware upgrades, units shipped from CyberData with firmware version 5.1.2 and later feature a built-in "fail safe" mechanism. Note that field upgrading earlier units with v5.x.x will not allow for this feature.

Note Any units that have shipped with firmware version 6.0.0 or later will not be able to run firmware that is version 5.1.2 or earlier.

Caution

When upgrading to firmware version 6.x.x from version 5.x.x or earlier, your device configuration settings will be lost because the way that the device stores the configuration settings is different in version 6.x.x.

To upload the firmware from your computer:

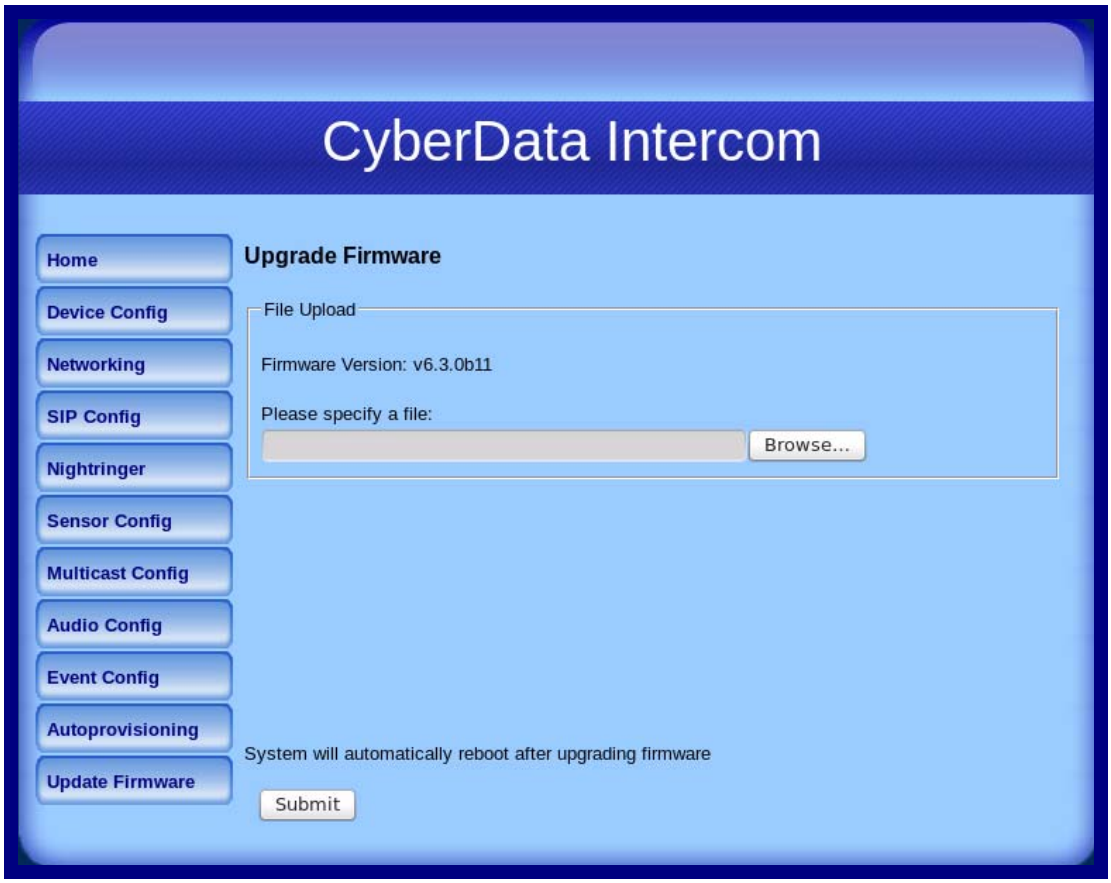
1. Retrieve the latest Intercom firmware file from the VoIP Intercom **Downloads** page at:
   http://www.cyberdata.net/products/voip/digitalanalog/intercom/downloads.html
2. Unzip the firmware version file. This file may contain the following:

- Firmware file
- Release notes

3. Log in to the Intercom home page as instructed in Section 2.2.2, "Log in to the Configuration Home Page".

4. Click the **Update Firmware** button to open the **Upgrade Firmware** page. See Figure 2-32.

Figure 2-32. Upgrade Firmware Page



5. Select **Browse**, and then navigate to the location of the Intercom firmware file.

6. Click **Submit**.

Note This starts the upgrade process. Once the Intercom has uploaded the file, the **Uploading Firmware** countdown page appears, indicating that the firmware is being written to flash. The Intercom will automatically reboot when the upload is complete. When the countdown finishes, the **Upgrade Firmware** page will refresh. The uploaded firmware filename should be displayed in the system configuration (indicating successful upload and reboot).

Table 2-18 shows the web page items on the **Upgrade Firmware** page.

Table 2-18. Firmware Upgrade Parameters

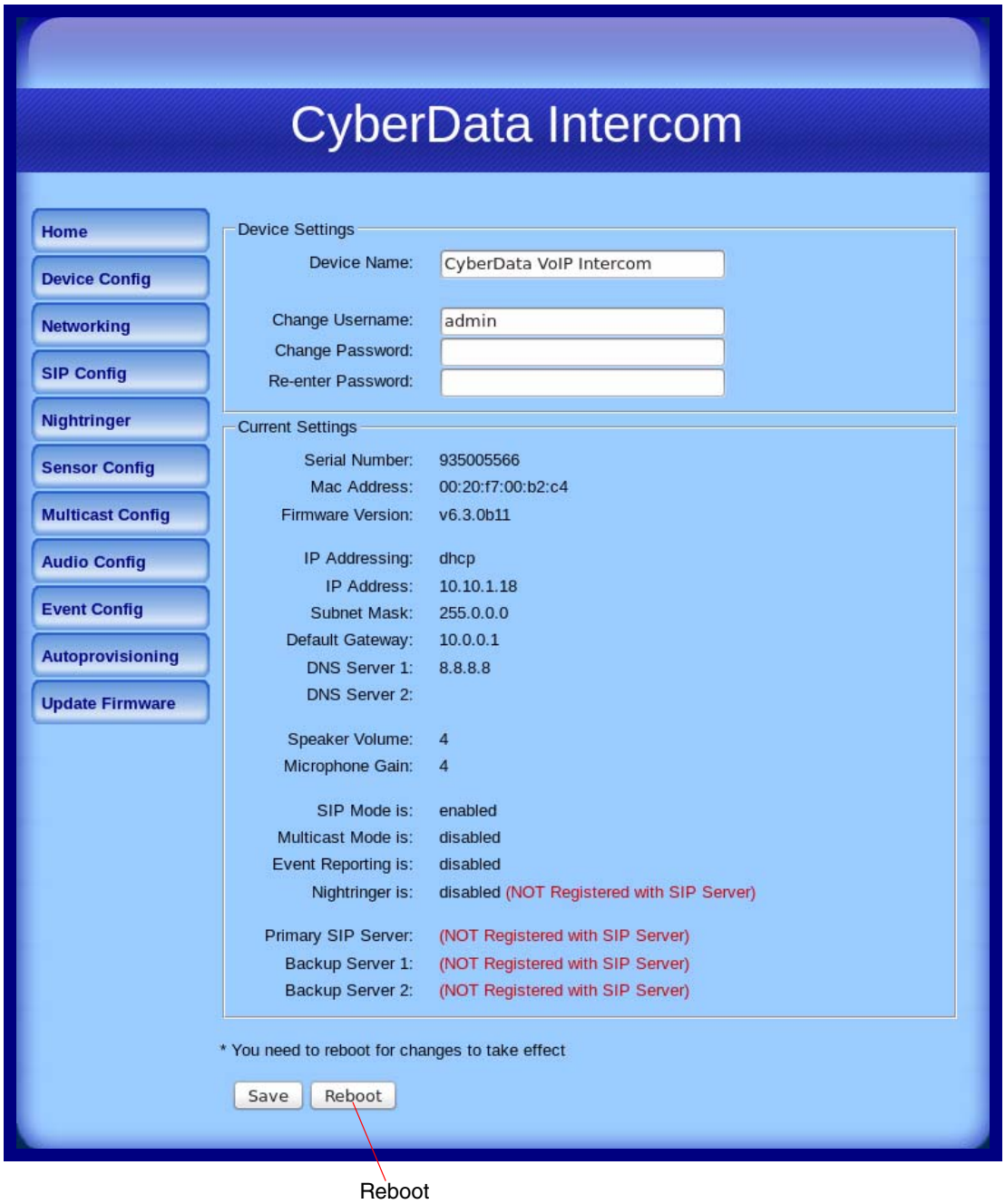
Web Page Item	Description
File Upload	
Firmware Version	Shows the current firmware version.
Browse...	Use the **Browse** button to navigate to the location of the Intercom firmware file that you want to upload.
Submit	Click on the **Submit** button to automatically upload the selected firmware and reboot the system.

2.3.1 Reboot the Intercom

To reboot a Intercom, log in to the web page as instructed in Section 2.2.2, "Log in to the Configuration Home Page".

1. Click **Reboot** (Figure 2-33). A normal restart will occur.

Figure 2-33. Reboot System Section



2.4 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in Table 2-19 use the free unix utility, **wget commands**. However, any program that can send HTTP POST commands to the device should work.

2.4.1 Command Interface Post Commands

Note These commands require an authenticated session (a valid username and password to work).

Table 2-19. Command Interface Post Commands

Device Action	HTTP Post Command[a]
Trigger relay (for configured delay)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "test_relay=yes"
Place call to extension (example: extension 130)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "call=130"
Place point-to-point call[b] (example: IP phone address = 10.0.3.72)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "call=10.0.3.72"
Terminate active call	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "terminate=yes"
Force reboot	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "reboot=yes"
Test Audio button	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "test_audio=yes"
Announce IP address	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "speak_ip_address=yes"
Play the "0" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_0=yes"
Play the "1" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_1=yes"
Play the "2" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_2=yes"
Play the "3" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_3=yes"

Table 2-19. Command Interface Post Commands (continued)

Device Action	HTTP Post Command[a]
Play the "4" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_4=yes"
Play the "5" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_5=yes"
Play the "6" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_6=yes"
Play the "7" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_7=yes"
Play the "8" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_8=yes"
Play the "9" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_9=yes"
Play the "Dot" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_d=yes"
Play the "Audio Test" audio file (from Audio Config)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_audiotest=yes"
Play the "Page Tone" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_pagetone=yes"
Play the "Your IP Address Is" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_youripaddressis=yes"
Play the "Rebooting" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_rebooting=yes"
Play the "Restoring Default" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_restoringdefault=yes"
Play the "Ringback tone" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_ringback=yes"
Play the "Ring tone" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_ringtone=yes"
Play the "Intrusion Sensor Triggered" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_intrusionsensortriggered=yes"
Play the "Door Ajar" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_doorajar=yes"

Table 2-19. Command Interface Post Commands (continued)

Device Action	HTTP Post Command[a]
Play the "Night Ring" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_nightring=yes"
Delete the "0" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_0=yes"
Delete the "1" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_1=yes"
Delete the "2" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_2=yes"
Delete the "3" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_3=yes"
Delete the "4" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_4=yes"
Delete the "5" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_5=yes"
Delete the "6" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_6=yes"
Delete the "7" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_7=yes"
Delete the "8" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_8=yes"
Delete the "9" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_9=yes"
Delete the "Audio Test" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_audiotest=yes"
Delete the "Page Tone" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_pagetone=yes"
Delete the "Your IP Address Is" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_youripaddressis=yes"
Delete the "Rebooting" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_rebooting=yes"
Delete the "Restoring Default" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_restoringdefault=yes"

Table 2-19. Command Interface Post Commands (continued)

Device Action	HTTP Post Command[a]
Delete the "Ringback tone" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_ringback=yes"
Delete the "Ring tone" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_ringtone=yes"
Delete the "Intrusion Sensor Triggered" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_intrusionsensortriggered=yes"
Delete the "Door Ajar" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_doorajar=yes"
Delete the "Night Ring" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_nightring=yes"
Trigger the Door Sensor Test (Sensor Config page)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/sensorconfig.cgi" --post-data "doortest=yes"
Trigger the Intrusion Sensor Test (Sensor Config page)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/sensorconfig.cgi" --post-data "intrusiontest=yes"

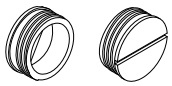
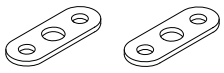
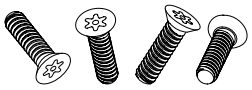
a.Type and enter all of each http POST command on one line.
b. Must be in point-to-point mode see Section 2.2.5.2, "Point-to-Point Configuration"

Appendix A: Mounting the Intercom

A.1 Mount the Intercom

Before you mount the Intercom, make sure that you have received all the parts for each Intercom. Refer to Table A-1.

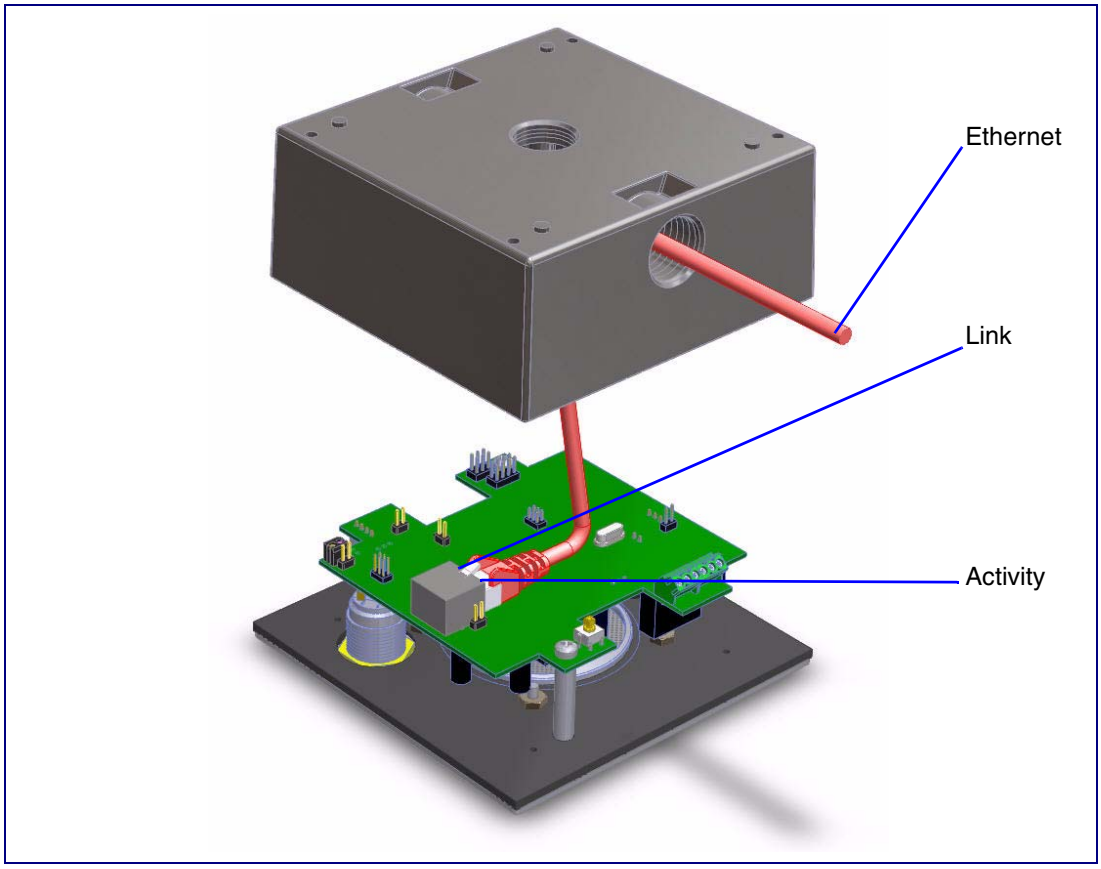
Table A-1. Mounting Components (Part of the Accessory Kit)

Quantity	Part Name	Illustration
2	Outlet Box Plugs	
2	Flush Mounting Plate	
2	8-32 x 1/4" Flat Head Phillips Machine Screw	
1	10-24 x 5/16" Pan Head Phillips Machine Screw	
1	T-15H Torx Key	
4	Security Torx Screw	

To mount the Intercom:

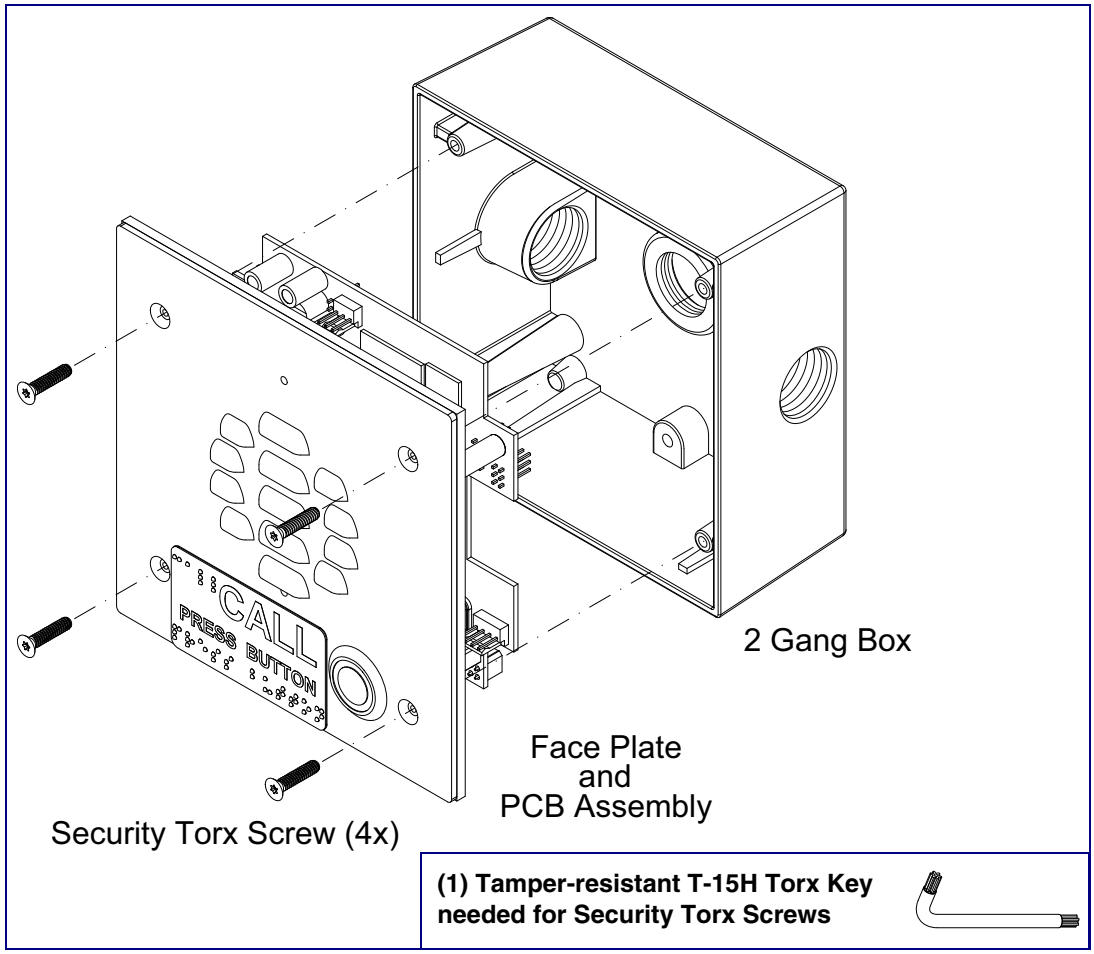
1. Plug the Ethernet cable into the Intercom Assembly (see Figure A-1). Section 2.1.5, "Network Connectivity, and Data Rate" explains how the **Link** and **Status** LEDs work.

Figure A-1. Network Connector Prior to Installation



2. To fasten the Intercom:
   - For wall mounting, use the two **8-32 X 1/4" FLAT HEAD PHILLIPS MACHINE SCREW** and the one **10-24 X 5/16" PAN HEAD PHILLIPS MACHINE SCREW** to secure the Intercom.

Figure A-2. VoIP Intercom Assembly



GENERAL ALERT

Caution

Equipment Hazard: Do not use an electric or power screwdriver to fasten the face plate and PCB assembly to the gang box. To prevent over-torque damage to the gasket, do not apply more than 10 inch-pounds force. Over-torquing will cause the gasket to tear, risk moisture intrusion, and effectively void the manufacturer's warranty.

If the thread on the conduit is longer than 3/8 inch, then a **stop nut** (not supplied) is required. Otherwise, use the **outlet box plug** to plug the exit hole.

Note Apply good quality waterproof sealant to all threads.

Figure A-3. Mounting the VoIP Intercom Assembly

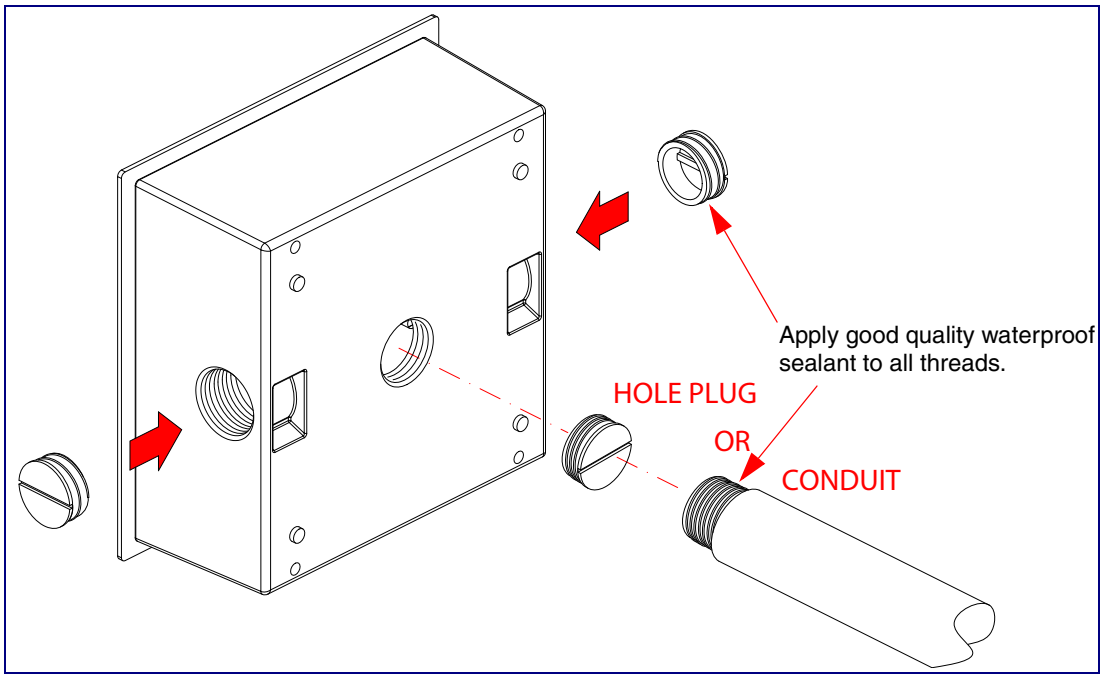


Figure A-4 shows the restrictions of the conduit going into the box.

Figure A-4. Conduit Restrictions

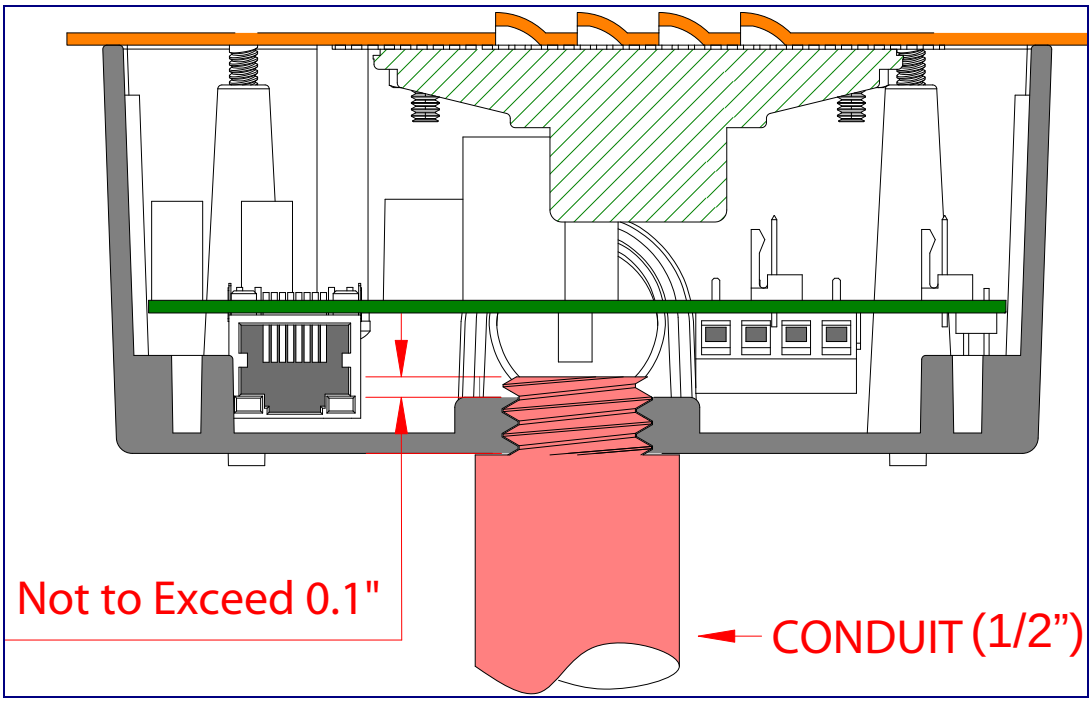
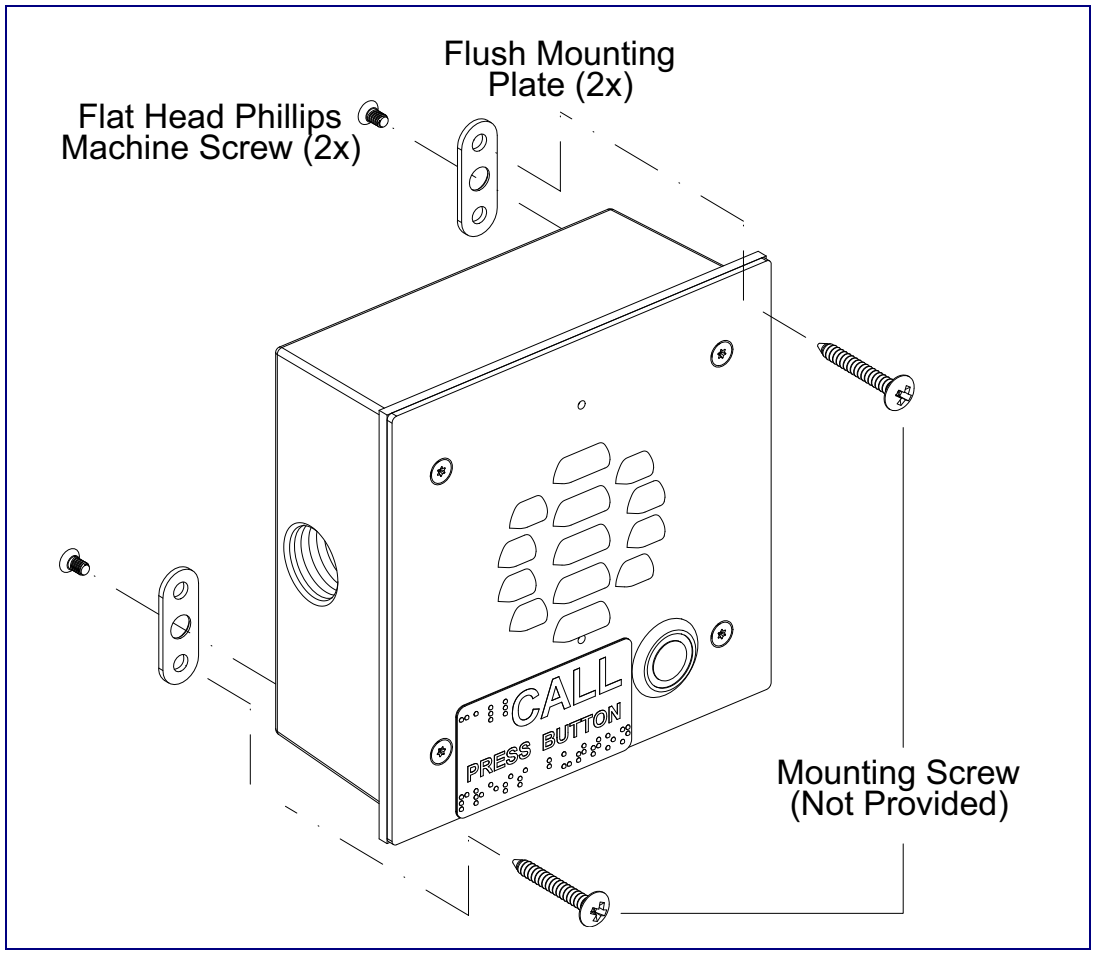


Figure A-5 shows how to properly mount the VoIP Intercom.

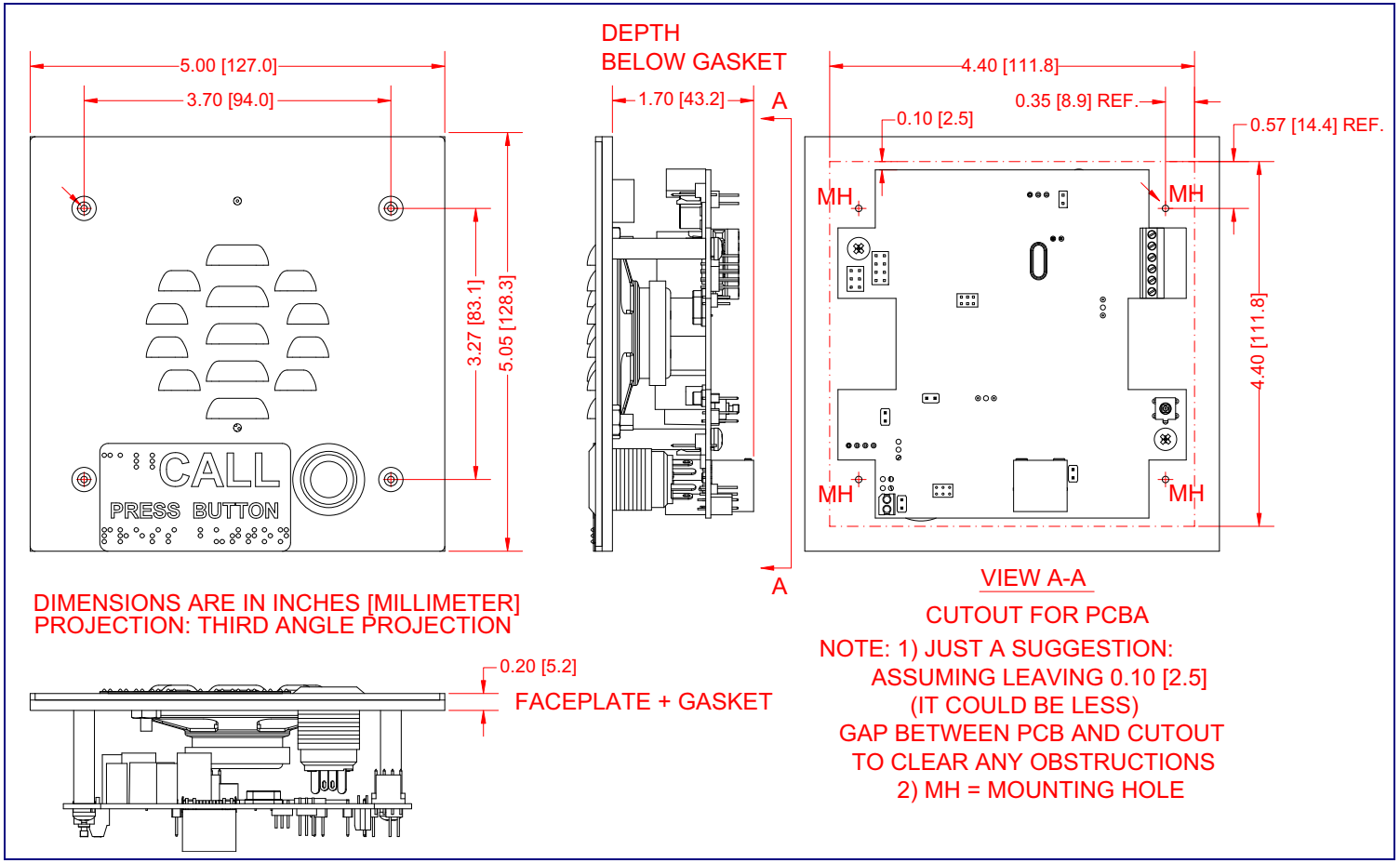
Figure A-5. Mounting



A.1.1 Custom Flush Mounting

Figure A-6 shows how to do a custom flush mounting for the VoIP Intercom.

Figure A-6. Custom Flush Mounting



Appendix B: Setting up a TFTP Server

B.1 Set up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

B.1.1 In a LINUX Environment

To set up a TFTP server on LINUX:

1. Create a directory dedicated to the TFTP server, and move the files to be uploaded to that directory.
2. Run the following command where `/tftpboot/` is the path to the directory you created in Step 1: the directory that contains the files to be uploaded. For example:

   ```
   in.tftpd -l -s /tftpboot/your_directory_name
   ```

B.1.2 In a Windows Environment

You can find several options online for setting up a Windows TFTP server. This example explains how to use the Solarwinds freeware TFTP server, which you can download from the following website address:

http://www.cyberdata.net/support/voip/solarwinds.html

To set up a TFTP server on Windows:

1. Install and start the software.
2. Select **File/Configure/Security** tab/**Transmit Only**.
3. Make a note of the default directory name, and then move the firmware files to be uploaded to that directory.

Appendix C: Troubleshooting/Technical Support

C.1 Frequently Asked Questions (FAQ)

A list of frequently asked questions (FAQs) are available on the VoIP Intercom product page at:

http://www.cyberdata.net/products/voip/digitalanalog/intercom/faqs.html

Select the support page for your product to see a list of frequently asked questions for the CyberData product:

C.2 Documentation

The documentation for this product is released in an English language version only. You can download PDF copies of CyberData product documentation from the VoIP Intercom product page at:

http://www.cyberdata.net/products/voip/digitalanalog/intercom/docs.html

C.3 Contact Information

Contact	CyberData Corporation 3 Justin Court Monterey, CA 93940 USA www.CyberData.net Phone: 800-CYBERDATA (800-292-3732) Fax: 831-373-4193
Sales	Sales 831-373-2601 Extension 334
Technical Support	The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website: **http://www.cyberdata.net/support/contactsupportvoip.html** Phone: (831) 373-2601, Ext. 333 Email: support@cyberdata.net
Returned Materials Authorization	To return the product, contact the Returned Materials Authorization (RMA) department: Phone: 831-373-2601, Extension 136 Email: RMA@CyberData.net When returning a product to CyberData, an approved CyberData RMA number must be printed on the outside of the original shipping package. No product will be accepted for return without an approved RMA number. Send the product, in its original package, to the following address: CyberData Corporation 3 Justin Court Monterey, CA 93940 Attention: RMA "your RMA number"
RMA Status Form	If you need to inquire about the repair status of your product(s), please use the CyberData RMA Status form at the following web address: **http://www.cyberdata.net/support/rmastatus.html**

C.4 Warranty

CyberData warrants its product against defects in material or workmanship for a period of two years from the date of purchase. Should the product fail within the warranty period, CyberData will repair or replace the product free of charge. This warranty includes all parts and labor.

Should the product fail out-of-warranty, a flat rate repair charge of one half of the purchase price of the product will be assessed. Repairs that are in warranty but are damaged by improper modifications or abuse, will be charged at the out-of-warranty rate. Products shipped to CyberData, both in and out-of-warranty, are shipped at the expense of the customer. Shipping charges for repaired products shipped back to the customer by CyberData, will be paid by CyberData.

CyberData shall not under any circumstances be liable to any person for any special, incidental, indirect or consequential damages, including without limitation, damages resulting from use or malfunction of the products, loss of profits or revenues or costs of replacement goods, even if CyberData is informed in advance of the possibility of such damages.

C.4.1 Warranty & RMA Returns within the United States

If service is required, you must contact CyberData Technical Support prior to returning any products to CyberData. Our Technical Support staff will determine if your product should be returned to us for further inspection. If Technical Support determines that your product needs to be returned to CyberData, an RMA number will be issued to you at this point.

Your issued RMA number must be printed on the outside of the shipping box. No product will be accepted for return without an approved RMA number. The product in its original package should be sent to the following address:

CyberData Corporation

3 Justin Court.

Monterey, CA 93940

Attn: RMA "xxxxxx"

C.4.2 Warranty & RMA Returns Outside of the United States

If you purchased your equipment through an authorized international distributor or reseller, please contact them directly for product repairs.

C.4.3 Spare in the Air Policy

CyberData now offers a *Spare in the Air* no wait policy for warranty returns within the United States and Canada. More information about the *Spare in the Air* policy is available at the following web address:

http://www.cyberdata.net/support/warranty/spareintheair.html

C.4.4 Return and Restocking Policy

For our authorized distributors and resellers, please refer to your CyberData Service Agreement for information on our return guidelines and procedures.

For End Users, please contact the company that you purchased your equipment from for their return policy.

C.4.5 Warranty and RMA Returns Page

The most recent warranty and RMA information is available at the CyberData Warranty and RMA Returns Page at the following web address:

http://www.cyberdata.net/support/warranty/index.html

Index

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

Y